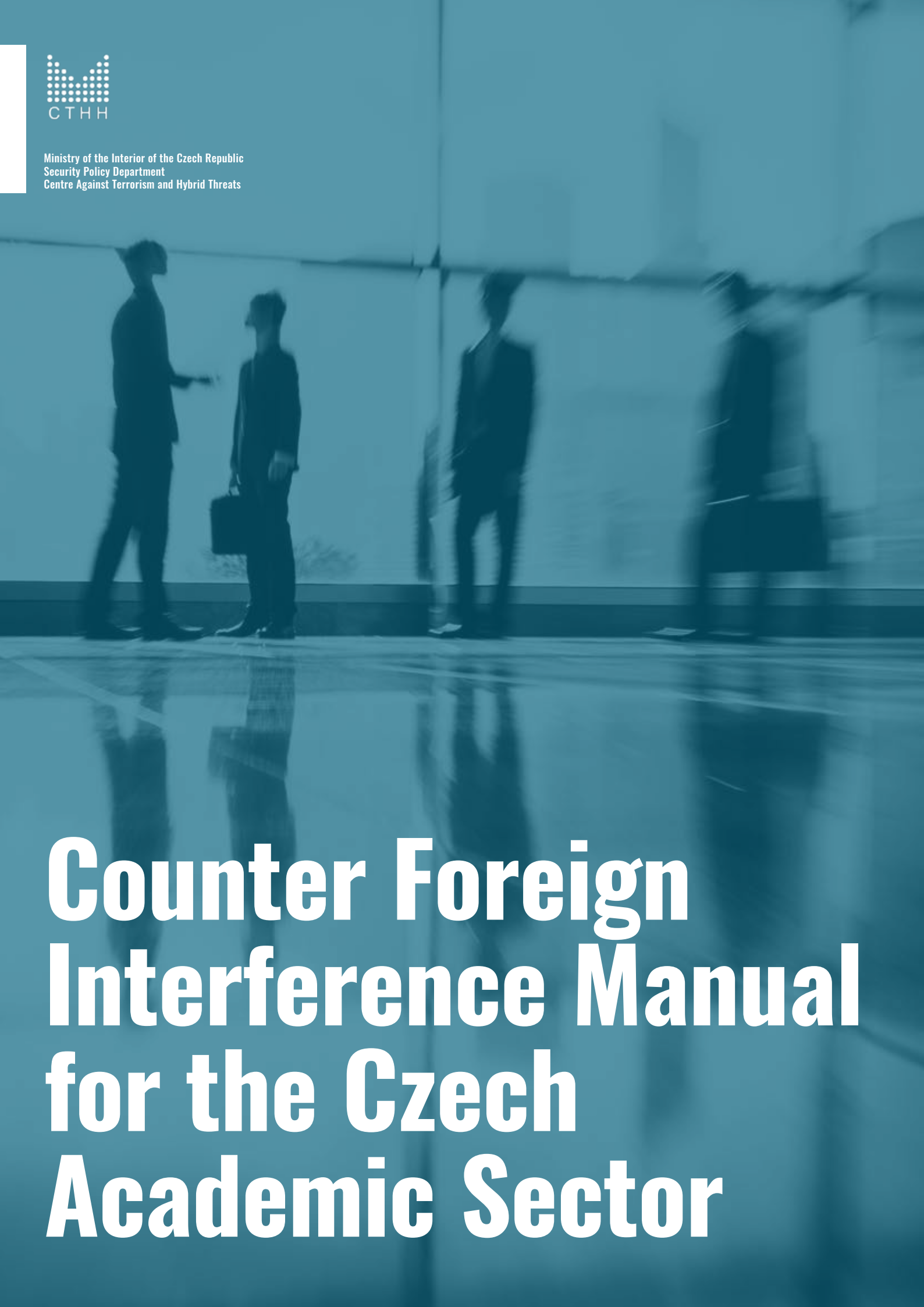


CTHH

Ministry of the Interior of the Czech Republic
Security Policy Department
Centre Against Terrorism and Hybrid Threats

Counter Foreign Interference Manual for the Czech Academic Sector

Content

1

Introduction

Distinguished members of the academic sector and non-academic members of higher education institutions, this document was created at the request of Charles University, spurred by recent events both in the Czech Republic and around the world, as it is becoming increasingly apparent that it is essential to systematically address interference attempts by foreign powers at universities.

An unquestionable part of Czech security interests is to have a flourishing and independent higher education sector that is able to exercise academic freedoms and rights protected by law, as well as to ensure the transparent financing of higher educational institutions (HEIs). Act. No. 111/1998 Coll., on Higher Education Institutions, defines academic freedoms and rights, which presume a high level of personal responsibility within academia, including the duty to protect these freedoms and rights. Interference operations run by foreign powers disrupt both the freedoms and rights significantly, and it is essential that protection against this interference is achieved through the personal responsibility of members of academia as well as standardized institutional measures on the part of universities.

The goal of this document is to **help you prepare for a situation in which you may become of interest to a foreign power and to help you learn how to respond to such a situation**. We want to acquaint you with the basic idea and general guidelines on how to take preventive action, which questions to ask yourself, what issues to cover by your internal rules, but also how to deal with situations that arise and how to build common know-how in cooperation with other higher education institutions **to increase resilience to the interference**.

The document is divided into two main parts. The first focuses on **setting up a system to increase resilience to interference**. The second **aims to indicate to individuals how the influence of foreign powers can affect them** and how they can defend themselves.

In no way is the aim to impose new legal or administrative obligations on universities; on the contrary – **the implementation of counter-interference measures resides on the principles of voluntariness and personal and institutional responsibility**. We fully respect the independence of HEIs and are aware that most of them already have internal security rules in place. Still, the threat of interference may not always be covered satisfactorily.

This document is primarily a **collection of advice and recommendations**, as well as a **guide** on how to deal with situations where interference is present, and on how to react and proceed. The text does not aim to be exhaustive in describing all the ways in which interference can affect HEIs and academia, but focuses on describing basic techniques and procedures. In practice, **it is apparent that it is not always possible to prevent all threats in their breadth and depth, but it is good to be aware of them and to prepare for them**.

We acknowledge that the reputation and success of our higher education system is based on its openness and independence. We encourage being open to different thoughts, ideas and trends, to students from different socio-economic groups and students from abroad, and being independent of the country's political system and the foreign interference.

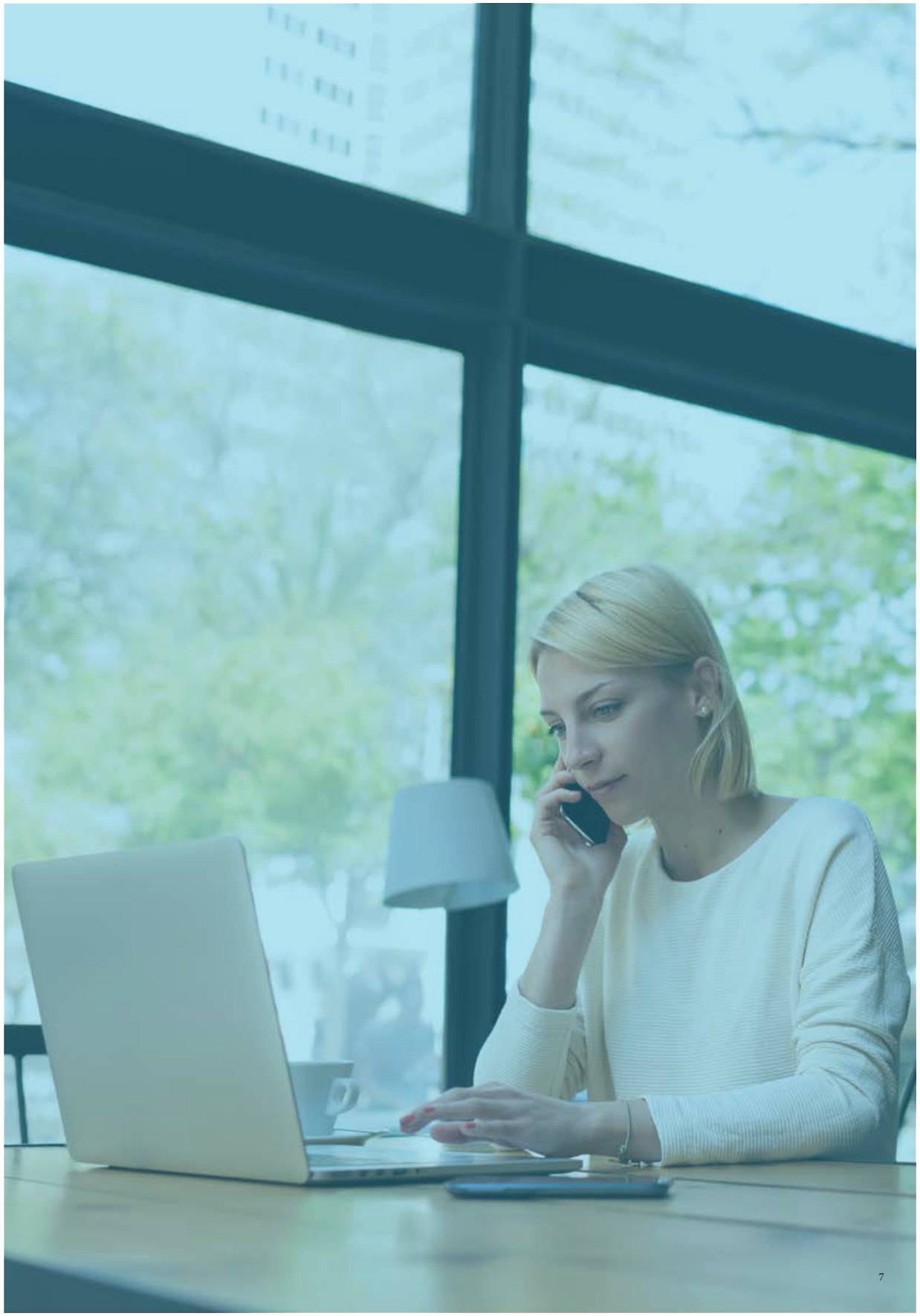
Cooperation with foreign universities, as well as other entities and organizations, is an integral part of today's complex academic world. In the absolute majority of cases, such cooperation is beneficial

and poses no additional risks or threats. However, in a globally interconnected environment, new challenges and threats arise that jeopardise, among other things, intellectual property and IT systems, but also the reputation of universities and their staff and legally protected academic freedoms.

The following text is based on documents produced on this topic by the European Union (specifically the European Commission[1,2], and the European Parliament[3,4]), national documents issued by the governments of the USA[5], the UK[6,7] Germany[8] and Australia[9], and several foreign universities.[10,11,12,13,14] The findings and recommendations of these documents were adapted to the Czech environment and enriched by the expertise and experience of Czech security professionals.

Basic principles upon which this document is based:

- Academic freedoms and rights are guaranteed by law, but this does not mean that they are sufficiently protected against the influence of foreign powers.
- Research, cooperation, contractual relations and educational activities must not contradict the Czech legal order.
- Security is a collective matter, but everyone has a certain degree of personal responsibility.
- Security requirements should be proportionate to the risks.
- Protecting the higher education sector and its values against inteference of foreign powers is important.



2

Definiton of Selected Terms

As this text aims to provide the reader with an elementary insight into the foreign interference with focus on the higher education sector, the reader must be familiar with the basic definitions of the terms used.

Considering that the interference can take various forms, many of which do not violate the applicable laws on the level of the individual steps, it is necessary to modify some definitions directly for purposes of this text.

Intelligence agent – A person knowingly, or possibly unknowingly, acting for the benefit of an intelligence service. They generally perform tasks assigned to them; they are not intelligence officers.

Academic staff – For the purposes of this publication, it shall consist of professors, associate professors, other scientific and professional staff and students.

Assets of a higher education institution (HEI) – In this case this shall not concern property, but primarily people (academic staff, researchers, PhD students, other students and employees), know-how, intellectual property, research projects, contracts with external partners, as well as the instition's reputation and position within the society and in the international context and the respect held by it.

Foreign power – The Czech legal order defines the term in Act No. 412/2005 Coll., on the Protection of Classified Information and Security Clearance, as amended, in Section 2, letter g) as follows: „Foreign power means a foreign state or its authority or a supranational or international organisation or its authority." For the purposes of this text, the definition shall be extended to include any other non-state actors (natural or legal persons), regardless of their nationality. Therefore, when „foreign powers" are referred to in this text, this shall mean both Czech and foreign natural and legal persons (e.g. governments, government authorities, Czech as well as foreign companies, political parties, etc.) that could in any way negatively interfere with the institution and its assets, including its reputation.

Due diligence – In this case, this shall mean the tracing of information on the subject of investigation (i.e. a foreign power representative) recordable in writing or another way and consisting, in the least, of freely available data from open sources, other academic or scientific databases, internal information sources of the HEI, and information and experience gained though cooperation among entities in the higher education sector and risk analyses resulting from acquiring this information.

Influence[15] – All actors seek to influence the debate on matters and issues that are important to them. If such activities are carried out in a legal and transparent manner (where these actors openly declare their intentions), then these are considered regular and common activities carried out by public and private Czech and foreign actors, for example as part of international relations, diplomacy, and PR, and they can make a positive contribution to the public debate.

Attacker – An entity exercising influence over a target person or institution, for example an intelligence officer, an agent of a foreign intelligence service, a lobbyist, or a representative of the private sphere trying to influence the target entity to act or not to act by using various influence techniques.

Interference – An undesirable and unacceptable form of influencing carried out by a foreign power or on behalf of a foreign power. This

form of influencing consists in particular of covert, deceptive, coercive or corrupt activities directed against the academic rights and freedoms and the interests of universities as well as their values and reputation (including the interest in having a robust, independent and transparently funded higher education system, etc.).

Higher education institutions (HEIs) – For the purposes of this document, the primary definition shall be the one in Act No.111/1998 Coll., on Higher Education Institutions, Section 2, Paragraph 3, Sentence 1: „Higher education institutions are universities or non-universities." However, where the term „higher education institution" i used, it shall also mean, for example, the individual faculties and other organisational units if applicable.

Intelligence activities – Sometimes also referred to as espionage. In academic and research environments, these activities focus mainly on the theft and transfer of know-how, gaining access to sensitive information, research project results, innovative solutions etc. Still, in some phases, they also often focus on gathering supporting information such as the atmosphere at the respective departments, the weaknesses and strengths of individual employees, workplace relationships, etc., ultimately allowing foreign powers to save time and resources.

Intelligence officer – A member of an intelligence service who may work under a variety of covert identities, e.g. as a diplomat, student, researcher, businessman etc., and who needs a variety of contacts and persons to be able to carry out his or her activities, using these contacts and persons in various ways to serve the interests of his or her country.

3

Why Is the Academic Environment Interesting to Foreign Powers?

When you enter an academic environment, you become a person with access to a range of sensitive information interesting for a foreign power. You often have access to the personal information of hundreds to thousands of students who are expected to become the nation's political, social, cultural, and business elite. Some of you have access to grants and research projects, or you can influence the content and format of lessons and courses. As academics, you are often part of the public and professional debate on a wide range of domestic and foreign policy issues. By the nature of your work, you maintain extensive contacts with colleagues at other universities at home and abroad. Many of you also have connections to active politicians, security forces, journalists and people from the business world. It is only natural that you have such access and contacts as they are essential to your work.[16]

The very cornerstone of the approach we want to present here is the mere awareness of what such information and contacts can mean to someone else and how a foreign power can use them.

What makes you a target of foreign powers' interests far more often than you think is your access to processes, functions and information that may represent a potential source of information for persons representing the interests of other states or non-state actors. These interests may not always be sympathetic to the Czech Republic or organizations of which the Czech Republic is a member.

Academia is a large source of information, much of which is sensitive by itself or in aggregate, classified or regulated by the state or by a contractual relationship with a partner.

The professional reputation and academic achievements of your institution are the results of the your and many of your colleagues' long-term work. **It is in your interest to help protect the reputation of your institution, your workplace, your intellectual property, and the information you possess and have access to. The actions and activities of each of you contribute to the protection of academic rights and freedoms, and other interests, which we strive to protect from the interference through our collective efforts.**

You matter.
You are important.

4

How to Set Up a Counter Foreign Interference System

HEIs conduct research in a wide range of disciplines like the arts, social sciences, medicine and engineering. The risk of interference varies from field to field. Furthermore, each department and area of focus within each field faces a different level of risk as well.

If a foreign power takes an interest in an HEI employee or student, **the target of that interest is most likely not the person as an individual but the information, access, or decision-making powers that the person possesses**. The goals of potential attackers may differ.[17] They may attempt to influence the teaching or part of it to fit a particular vision of the world. Attackers may want to find out what you do in your workplace or gain potentially helpful information through you in the future. In the case of basic or applied research, attackers may then want to gain access to the results of that research, saving their company or country thousands of hours of research, failures, searching for alternative solutions, as well as considerable financial resources.

Potential attackers do not necessarily have to be memebers of a foreign intelligence service. They can be, for example, a company interested in obtaining contracts, a person asserting its interest in changing a decision issued by your department, or an entity engaged in collecting information that could be monetized in the future. They can be a hacker who is just having fun, but should they come across interesting information from your databases, they may try to monetize it. Hacking attacks can also be targeted. The attacker may even hire a hacker if their IT skills are not up to the necessary level. Some individuals and companies steal others' information on commission or for future use. **Information from HEIs and their legal entities founded or owned by them is valuable and can undoubtedly be exploited in the future.**

Basic procedures to mitigate the risk of foreign influence should include the measures detailed in the following chapters:

- Risk Management
- Due Diligence
- Communication and Training
- Sharing Know-How
- Cybersecurity

4.1
Risk Management

Identifying and managing risks is key to reducing the risk of interference in the higher education sector (and elsewhere). The aim then is to apply risk management processes to reduce vulnerability to interference in all activities of HEIs or to mitigate such interference. In particular, the most attention should be focused on:)

- Protecting intellectual property, research projects and grants, their content and progress,
- Protecting the reputation of the HEI, members of the academic community, partners and other stakeholders,
- Watching out for the risks that partners and external (off-budget) funding may present.

HEIs management is responsible for analysing security risks and developing strategies to mitigate them. A robust security policy must be based on active management, communication and the realisation that security is a long-term goal that can only be achieved through systematic and continuous work. To create it, it is necessary to continuously analyse existing risks, which change over time and with the circumstances, and to set up measures to reduce them, communicate about these measures, implement them, and evaluate their effectiveness.

Questions that university management should ask themselves:

- Who in the HEI's management is responsible for assessing the risk of interference and for applying appropriate countermeasures?
- What internal rules, guidelines or regulations do you have that address the existence of the risk of interference and how do these documents help managers, employees and students understand who, what, when and how is at a higher risk of interference?
- How exactly are the risks of each research project analysed? Do you have a central oversight set up to assess the potential risks in addition to the scientific benefits?
- Do you have minimum due diligence requirements?
- Do you train employees and others (e.g. selected students) to increase their resilience to interference? Is the scope of training sufficient?
- Do you have an internal communication system in place to report incidents so that they can be evaluated and adequate countermeasures can be taken?
- How are internal rules set up to deal with incidents of suspected interference? Who handles these incidents? What are the procedures and tools for doing so?
- Who is to decide on the initiation of cooperation with the security forces or responsible ministries should you discover a possible interference and when is the decision to be made?
- Do you have a communication strategy and communication plans in place both within and outside your institution, including procedures for situations where interference is present?
- Do you incorporate lessons learned from evaluated incidents into your internal policies, procedures, regulations and training? Do you share lessons learned with other colleges?

If you are not sure about the answers to the above questions or if you have answered some of them with a no, then it is advisable to work on measures to counteract the interference at your institution. **Decide to whom in top management you will assign the agenda of protection against interference.** Recognise that even within a single institution, there are projects, faculties, departments and other units where **the risk of interference varies considerably.**

Conduct an analysis of your institution's assets to identify which of your employees could become targets of interference, particularly concerning decision-making powers and access to information about, for example, students, staff and research projects, but also about access to the media, political parties, security forces and the business community. Do the same where students are concerned, for example according to what subjects they are studying.

Following these steps, **analyse your existing strategic documents, security rules and processes and identify how they address the protection of people, information and IT systems**. Integrate the risks of interference among the risks you are considering. Establish processes to **identify** areas of your business with increased risk of interference, **set sufficient countermeasures to mitigate these risks, and establish standard procedures to address such situations**.

These measures should always include minimum due diligence requirements, **a proactive and robust communication strategy inside and outside your school**, and a system of training for the management, staff and students. Each group may require a different scope of training.

In most cases, it is not necessary to give up working on a project or cooperating with a partner where you identify an increased risk of interference. You can resolve the situation, for example, **by setting up more robust control mechanisms**, more frequent audits of the project and its benefits, contractual restrictions on the partner's activities and authorisations, etc.

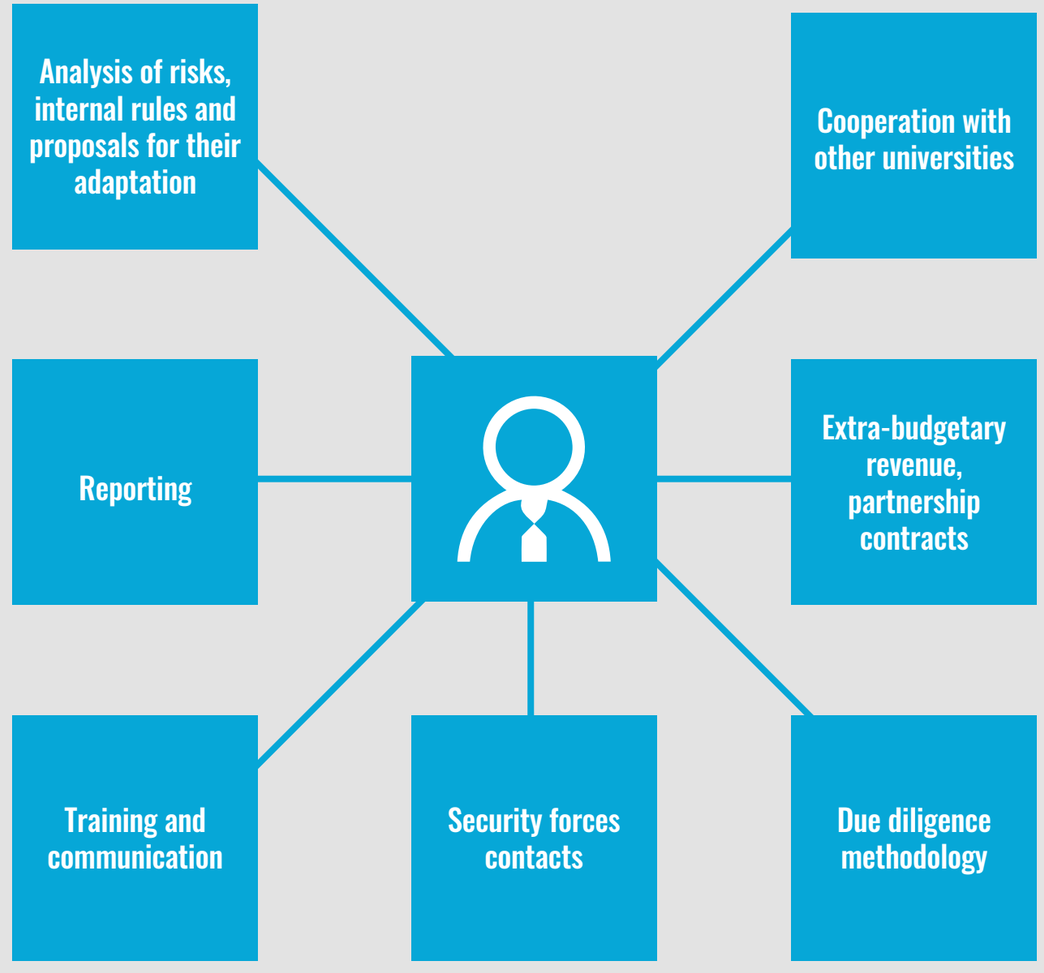
Internal rules and guidelines should specify the requirements for individual stakeholders and entities that need to be applied in case of cooperation with a foreign power. **Standard procedures implemented to detect the potential risk of interference must be clearly defined at all management levels, and responsibility for their implementation must be clearly established**.

An internal reporting system of security incidents and its appropriate setup, when used long-term, allows for an easier assessment of the risks that occur most frequently in your work, including where the measures you have set up to eliminate and reduce them are working and where they are not.

The roles and responsibilities of managers with regard to cooperation with foreign powers should be clearly and distinctly defined. Primary policy documents describing the rules and responsibilities for the university's collaboration with foreign powers should be written so that their interpretation is clear and that they provide clear instructions on how to proceed and what to avoid. They should also include procedures to reduce the risks posed to the university when cooperating with a foreign power.

An important element of the whole process is also the preservation of documentation related to assessing the risks of interference for each individual entity (project, workplace, cooperation agreement, etc.). Similarly, store documentation covering the decision-making process on the measures taken. Such **documentation provides a fundamental retrospective view**, especially considering that any given risk may be assessed differently before and after a potential incident. This implies that a responsible person in the management of the HEI should be appointed to head the whole process, from continuous risk assessment through checks on compliance with the set measures and training of the persons involved to the archiving of all documentation showing the above steps. Ultimately, however, it is always up to the HEI whether it adds these tasks and the responsibility for their implementation to the agenda of a manager, provides a manager with a team of people depending on the scope of the work envisaged, or sets up a group of people responsible for the implementation of these tasks.

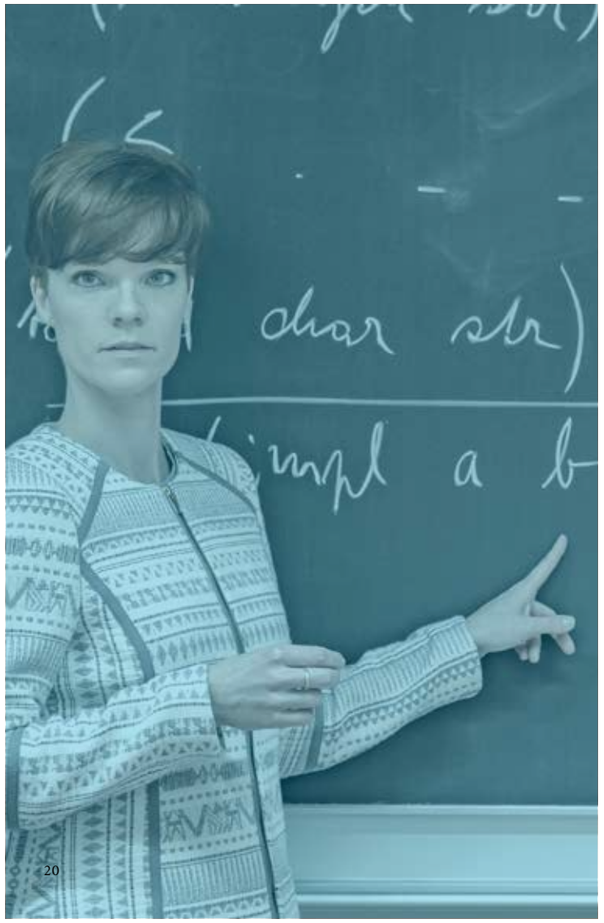
Tasks of the responsible manager



4.2
Due diligence

HEIs need to know their partners, not least because they may in some cases be at risk of interference. **The 'know your partner' principle should be applied as widely as possible to minimise this risk.**[18] This principle needs to be applied so that, as part of the process of vetting the partner and their credibility, the university and its representatives come to know the partner sufficiently **before** any formal cooperation is established.[19]

Collaboration between HEIs and third parties is based on a combination of formal and informal links with foreign and local partners. The absolute majority of this cooperation is beneficial and desirable from the point of view of the institutions themselves and the Czech Republic and shows no signs of interference. This is a state of affairs that is very much supported and desired both by the state and society.



Academics and other staff in the higher education sector have a duty to act according to the laws of the Czech Republic and the internal regulations of their employer. **Internal documents and rules that alert them to the risks of interference and the procedures to counter them will make it much easier for them to meet their obligations to protect the academic rights and freedoms and independence.**[20]

In any partnership, the extent and degree of risk of interference depends to a large extent on the nature of the joint activity to be undertaken. In many cases, specific legislation or other contractual conditions also play a role.

The risk of interference can also evolve and change over time. Therefore the process of assessing this risk should be repeated for partners with whom universities enter into long-term partnerships. However, it is not possible to determine precisely how frequently it is appropriate to repeat the process. A reasonable recommendation seems to be to carry out a review **once every one to two years or whenever there is a significant change in the terms of cooperation or when there is a new piece of information** that could impact the risk assessment. The 'know your partner' principle should always be followed to the extent necessary to assess the risk of interference, and based on the cooperation's time frame, nature, and scale, it should be assessed whether the pros outweight the cons or vice versa. Consider including a possible outlook for the evolution of the risk of interference, at least for the medium term.

In the meantime, **there may also be changes in regulatory requirements by the government or the grantor**. New rules may be set, but also, for example, sanctions may be imposed on some of the entities with which your institution has cooperated so far. In such a case, it is necessary to react to the newly created situation and not only to modify the internal documents related to reducing the risk of interference but also to make subsequent modifications in the affected contractual relations, e.g. in the form of an amendment to the original contract, without undue delay.

HEIs should also be mindful of the financial risks of working with a foreign power and should manage and mitigate these risks. They should also consider steps to assess potential reputational, political, security and other risks associated with, for example, staff, sponsors, visiting academics and research projects, and then make decisions based on an assessment of these risks as well. The risk analysis should consider that many foreign collaborators may have undisclosed relationships and commitments or may not fully know and respect the rules that Czech HEIs are obliged to follow.

The HEI's management should ensure that its **employees are trained in, at the very least, the basics of recognizing interference and the proper procedures for dealing with suspicions that such interference is occurring**. For academic and research staff who are identified by HEI management as being at increased risk of malign foreign influence, the training should be more in-depth. Such training should be repeated regularly at predefined intervals. We see it as optimal to provide training once a year to HEI management and those with an identified risk of malign foreign influence, while once every two years is sufficient for others. The minimum scope of the training should include familiarisation with internal documents, rules and processes to limit the interference, instructions on how to proceed in specific situations, familiarisation of trainees with basic influence techniques they may encounter (within the scope of this material), and finally case studies and experience gained from the implementation of counter-influence measures.

4. 2. 1
Partnership Agreements and Cooperation with Foreign Powers

The absolute majority of contractual relationships with other entities in the higher education sector as well as with entities outside the sector and foreign entities are beneficial and contain very little risk of interference.

In the context of partnership and other agreements with domestic or foreign private entities or state, parastatal or non-state entities from third countries, it is advisable to seek answers to some critical questions before signing such agreements, thereby performing a thorough analysis. It is necessary to evaluate the positives and possible negatives and find out whether such a contract will be beneficial for your institution

and what threats and risks it entails. Very rarely is anything black and white. Most of the time, you will face a situation where you will need to assess whether the positives outweigh the negatives or vice versa. It is also to be expected that such assessment will become increasingly more demanded by academics or by the media and the public.[21]

Before formally signing a contract with a foreign power, the HEI should conduct due diligence on the partner entity. Similarly, the scope and extent of the cooperation should be precisely specified, including, for example, the provision of information or guarantees by the partner entity that could affect the assessment of the risk of interference.[22] These and other legal conditions (e.g. the obligation to respect human rights and freedoms, the Czech legal order, and academic freedoms) can be negotiated with future partner entities in the form of contracts on future agreements or memoranda of understanding with clear consequences for their breach.

Here are some of the questions you should ask yourself before signing any partner agreements:

- What information do you know about the partner entity? Are there indications of any suspicions? Is there information about contacts and connections that the partner should not have? Are the institutions or entity with whom you are about to enter into a contractual relationship trustworthy? Is there publicly available information about the activities of said entity or institution that could pose a future threat to the independence, reputation, or other interests of your university?
- Does the partner strive for transparency, or are there doubts, secrecy and ambiguities surrounding its functioning? How transparent is the partner in disclosing information about its other collaborating entities, owners, and intentions that your university should know about in advance? These may include existing relationships with the private sector, other universities and research institutes, and some government institutions at home and abroad.
- Does the contractual partner insist that all or part of the contract be kept private? This is understandable for some very specific projects where classified information or trade and other secrets are involved. Everywhere else, academic institutions should strive for as much transparency as possible to prevent problems.
- Does the contractual partner require the mutual agreement to contain passages not regularly included in this type of agreement? For example, does the partner insist that the contract contain various foreign policies or other declarations? Consider whether the declarations and statements in question are within the remit and interest of your university or whether they belong to the remit of a governmental body and whether their inclusion in the contract you are negotiating is necessary. Consider and find out why the partner wants them included in the contract.
- Does the contractual partner have an interest in influencing the topics of discussion on campus? Do they want to handpick teaching materials? Do they want to choose the topics of lectures and seminars? Do they have an interest in not discussing specific topics or only discussing certain topics in certain ways? Do they allow dissenting opinions or explanatory comments, e.g. from lecturers or other experts? Do they want to determine who will lecture and who will not?
- Is there an effort by the partner entity to negotiate a contract with your institution that is difficult or impossible to terminate in situations where, for example, academic freedoms or the ethics code is restricted or where it becomes known that the partner entity has become subject to export controls or sanctions? What situation will you find yourself in if any of the serious negative facts mentioned above are discovered? Will you be able to terminate the contractual relationship without significant losses?
- Does the contract comply with Czech law, or is the partner insisting that it should comply with the law of his home state? If so, it is worth examining whether or not such a section in the contract contravenes the fundamental human rights and freedoms guaranteed by the Charter of Fundamental Rights and Freedoms or restricts academic freedoms guaranteed by Section 4 of Act No. 111/1998 Coll., on Higher Education Institutions, or contravenes another part of the Czech legal order.

Always consider what you are offering and what you will get in return.[23, 24]

Governments in the US, Australia and the UK have already started to issue methodologies and recommendations to their higher education sectors to make it easier for them to identify risky behaviour by their partners.[25] For example, the UK government has issued a warning that "research collaboration with institutions originating from countries ruled by authoritarian regimes may be vulnerable to abuse by organisations and institutions operating in countries whose democratic and ethical values are different from our own".[26]

Among others, **sanctions lists announced by the Czech government, the EU or the UN** can be of assistance. These lists typically include individuals, groups, and organizations that have been or are involved in human rights violations, illegal arms trafficking, terrorism, or acts of extraterritorial violence. Various websites can serve as a primary source of information on sanctioned entities – the Ministry of Foreign Affairs's[27], the Ministry of Trade and Commerce (Licencing office)[28] or the Financial Analytical Office.[29] You can also use the website of the American NGO initiative Organized Crime and Corruption Reporting Project[30], the U.S. Senate staff report of China's impact on the U.S. Education System[31] or studies of the Australian Strategic Policy Institute.[32,33,34] Universities should also pay increased attention to contracting with politically exposed persons as well as financial institutions.

4. 2. 2
Donors and Financial Partners

Funding is one of the many ways in which foreign powers can exert their influence over HEIs. For a foreign power, it is a relatively easy and effective option. It can target an individual, a research team, a faculty, or an entire institution.

A foreign power may be interested in funding a research project or field of study. They may provide your institution with a sponsorship, offer a financial partnership or a grant. In return for such an investment, the foreign power expects, in the least, a positive impact on its reputation. Still, often the power is also interested in influencing the content of teaching or the output of scientific research to suit its interests. The foreign power may not seek to influence the entire institution or its organisational unit financially, but may focus its attention solely on individual members of the academic community and others in the higher education sector.

Always look for an answer to the question of who is the person or entity providing funds.[35] You need to conduct a full risk analysis of such a person or entity to determine whether it is an entity that could cause reputational or other problems for your university in the future.[36, 37] Keep in mind that the transparency of your university's funding is one of the most important parts of its reputation.

Another appropriate measure is to create a **register of all non-budgetary financial income** of your institution (you do not need to include student fees for extra study time or fees for self-paying students, money received from the Grant Agency of the Czech Republic[38], Technology Agency of the Czech Republic[39] or individual ministries and government bodies[40]). Ideally, it should record all income to the institution coming from outside sources. Such a register should be set up at the Rector's Office (at the top management). It should also include information on what steps have been taken in vetting the contributor or donor and a record of the process of approval of that financial income by your institution. This register can also be used to analyse part of the financial flows, but also, for example, to check whether similar financial contributors have been subject to comparable due diligence.

Expect that with the creation of transparent rules for accepting funds, some potential attackers will move from a position of seeking to engage on a more official level to a position of seeking unofficial contacts with individual employees.

Questions to ask when it comes to your university's off-budget resources:

- What internal policies and procedures are in place for receiving funding from sources outside the institution? Who is responsible for their implementation? The approval process should not be in the hands of one person, but should involve multiple people (3 is a good minimum).
- Have you created a register of all of your institution's financial income coming from foreign powers?
- Is there an apparent disparity between the performance required and the financial reward for the work done? If so, this may signal an attempt to discredit the recipient of the money or to set up for the blackmail of the recipient in the future.
- Does the payer (donor) require any non-standard sections to be included in the contract? Does the donor want to contractually ensure behaviour or its absence that is in contradiction with the Czech legal order and legally guaranteed academic freedoms?

4. 2. 3
Research and Intellectual Property Protection

Research is a powerful driver of growth in modern economies. This also reinforces its importance to foreign powers that may try to compromise the integrity of the system, but also some specific research projects.

HEIs usually have a system in place to protect their intellectual property. However, there is a need to analyse whether this system is also sufficiently responsive to the threats and risks to research activities and the protection of intellectual property arising from the interference.[41] Again, the process of identifying and managing risks is key to limiting the interference. HEIs should apply a risk management system to minimise the impact of interference on their research activities and protect the intellectual property they generate. In doing so, **the assumption is that risk perceptions and levels may differ significantly before and after a potential incident**.

One way foreign powers can secure access to, and in some cases influence over, research projects and intellectual property is through various forms of funding agreements, sponsorships and donations.[42] Another way is to attempt to win over members of research teams or administrative support through donations, bribes, blackmail or data theft.[43]

Therefore, check your university's rules for identifying such research project contracts that need more attention, especially where the research subject and/or the type of partnership is concerned. It is desirable that these rules are unambiguous and do not allow for alternative interpretations. When entering into contractual partnerships for research projects carried out in collaboration with foreign entities and/or the private sector, the requirements for risk analysis must also be clearly set out. The person responsible for implementing and updating them as well as training target persons on their content must be clearly identified.

However, there are other things to consider in connection to the risk management of research projects. For example, **it is not always possible to predict all possible variations in the future use of research results**. However, the risk management strategy should also include **steps to identify and protect potentially sensitive research and resulting technologies**. Much of the new knowledge, technologies, but also software can serve as so-called dual-use goods, and these are subject to stricter regulation by the state and the EU (see e.g. Act No. 594/2004 Coll.) implementing the European regime for the control of exports of dual-use goods and technologies[44]). Other research and technologies may have future military applications[45]. In such cases, these projects should always be given increased attention and protection.

It is also apparent that research with a future broad commercial application may face increased interest from foreign powers, whether from various private entities or foreign intelligence services. Correctly set rules and their application are crucial to identifying weaknesses in the protection of intellectual property and reducing the risk of its loss, misuse or theft.

4.3
Communication and Training

The nature of the higher education sector can offer many entry points for interference. HEIs should, therefore, proactively **provide training** to their staff and, in some cases, students to provide them with information on what interference can look like and **how to prevent it**.

Such training should include **guidance on what to do** if they believe they have observed an attempt to exert interference, whether on their own person, a colleague, a research project, a faculty, or the university. This proactive approach should include **an elaborate feedback system**. A system in which a reporting person sends in a complaint without receiving feedback will never work in the long run. The responsible official should contact the reporting person, arrange a personal interview, fill in other details that, for example, the reporter did not think to tell but may be very important to resolve the situation, provide information on how to proceed, and provide the reporter with at least basic guidance and advice on how to proceed in the situation. Especially in some evolving cases, it may be appropriate to repeat this procedure after some time. Later on, it is appropriate to inform the reporter of the conclusions and lessons learned or, if possible, the overall resolution of the case.

Each such case should also serve **to repeat the risk analysis**, in particular to discover whether your procedures and rules are applicable to the case in question and to correct them if they are not. The cases should then be included in subsequent staff and student training to reduce the likelihood of recurrence. Subsequently, such cases should be communicated to other HEIs so that there is a **desirable multiplication** of experience and to reduce the possibility of the same problem recurring at other institutions. It is quite common for an attacker to use the same modus operandi of attack against other universities. In some cases, it is appropriate to warn others at an early stage of the incident to create widespread awareness of the problem, with conclusions and lessons to follow later.

Rules in the following areas should clearly be part of the whole **system of training to increase resistance to interference**:

- Ethical rules for formal and informal meetings with representatives of foreign powers, including rules for social occasions and for accepting gifts, as well as for transparency about these contacts,
- Recommendations for safe travel abroad[46,47,48]
- System of access to individual workplaces as well as to individual IT systems used at your university,
- Rules for student activities at your institution (and on campus) to protect all students from interference with their academic and human rights and freedoms.[49]

Look for answers to the following questions:

- What training does your institution provide to increase resilience to interference? Is the format in terms of content and time sufficient for each group of trainees according to the level of risk determined by the interference risk analysis?
- What procedures do you have in place for reports of suspected or identified interference made by students, staff and others? Who reports what, to whom, when, and to what extent? What does such reporting look like? What is then done with each report? Do you have a set feedback loop for the reporter? Do you use your findings and lessons learned as well as those from collaborating universities?
- How can your institution's current internal policies on, e.g., ethics, social events, recommendations for safe travel, access to individual workplaces, information systems and the internet, be redefined or expanded to include solutions to facilitate the identification of potential risks of interference?
- How can your institution further support researchers and academics in their efforts to proactively manage the risk of interference, particularly where you identify an increased risk?

Another appropriate measure is a **detailed communication plan**, which should address who communicates what, to whom and at what time. This will limit situations where it is not clear who should communicate an event to staff and students, but also to the public if it is a case where the public should be informed. Appropriate and adequate communication is an integral part of dealing not only with matters relating to interference. Even a simple statement such as, "So and so has happened, we are dealing with the situation, we cannot say anything further at the moment" is better for the institution and its long-term reputation than silence, which gives room for various fabrications and sometimes even conspiracy theories.[50]

Some tips to consider:[51]

For external communication with the public, media and other HEIs

- Allocate sufficient people and resources for communication activities.
- Clarify how and through whom you want to receive information (information flow in) and how you want to inform external actors (information flow out).
- Always consider social networks; use their power and reach to your advantage. Try to avoid the spread of hoaxes and fake news that can harm you. In the aftermath of an incident, they are very likely to be present in the information space.
- The initial reporting may be brief – there will be time for details and analyses later.
- To communicate with the public, ideally prepare message texts for different types of incidents in advance and then adapt them to the specific situation. This will save time and prevent possible communication errors.

For internal communication with academic staff, students and other employees

- Make it clear in advance how you want to communicate with this group of people. Also inform them about how you as an organisation will proceed in the post-incident phase and what kind of communication they can expect. The initial reporting does not need to be extensive; there will be time for details and analyses later.
- Choose a communication tool that is reliable, that you know how to use, and that you trust to relay the information you are trying to communicate to the recipients.
- Consider the most effective ways to communicate. For example, calling academics, students or other staff into a conference room and informing them of the next steps directly may be a better solution than sending an email or making a phone call in some situations.

4.4
Sharing Know-How

As in other areas of activity, HEIs should **share their knowledge and experience relating to the ever-evolving risk of interference**. This includes the debate on the creation of indicators used at a given institution to detect the interference, as well as the approach to risk management, the training system and work with the reports, as well as adjustments to the rules of external funding of research and teaching, the rules for economic activity of employees outside the performance of work for their employer in academia and others. Such information exchange should also include sharing specific knowledge on detected interference, as well as mutual information on how individual incidents are handled, case studies, and analyses. The exchange of such knowledge should occur, for example, in a working group meeting or through a defined online platform within a university or research institution and across the higher education sector.

Where there is suspicion of a violation of the law that cannot be resolved by an internal act of the management, or the procedure under the Labour Code (Act No. 262/2006 Coll.), it is necessary to contact the Police[52] or the Security Information Service[53] and ask for help. A proactive approach to addressing the risk of interference is the key to reducing any individual attacker's influence operations.

4.5
Cybersecurity

Cybersecurity is an integral part of the mixture of measures to reduce the risk of interference. **Indeed, a significant part of the interference is linked to the cyber world**. Theft of data or breach of its integrity or disruption of the availability and reliability of IT networks are among the techniques of interference.[54] HEIs should therefore also focus their attention on improving their approach to cybersecurity.[55]

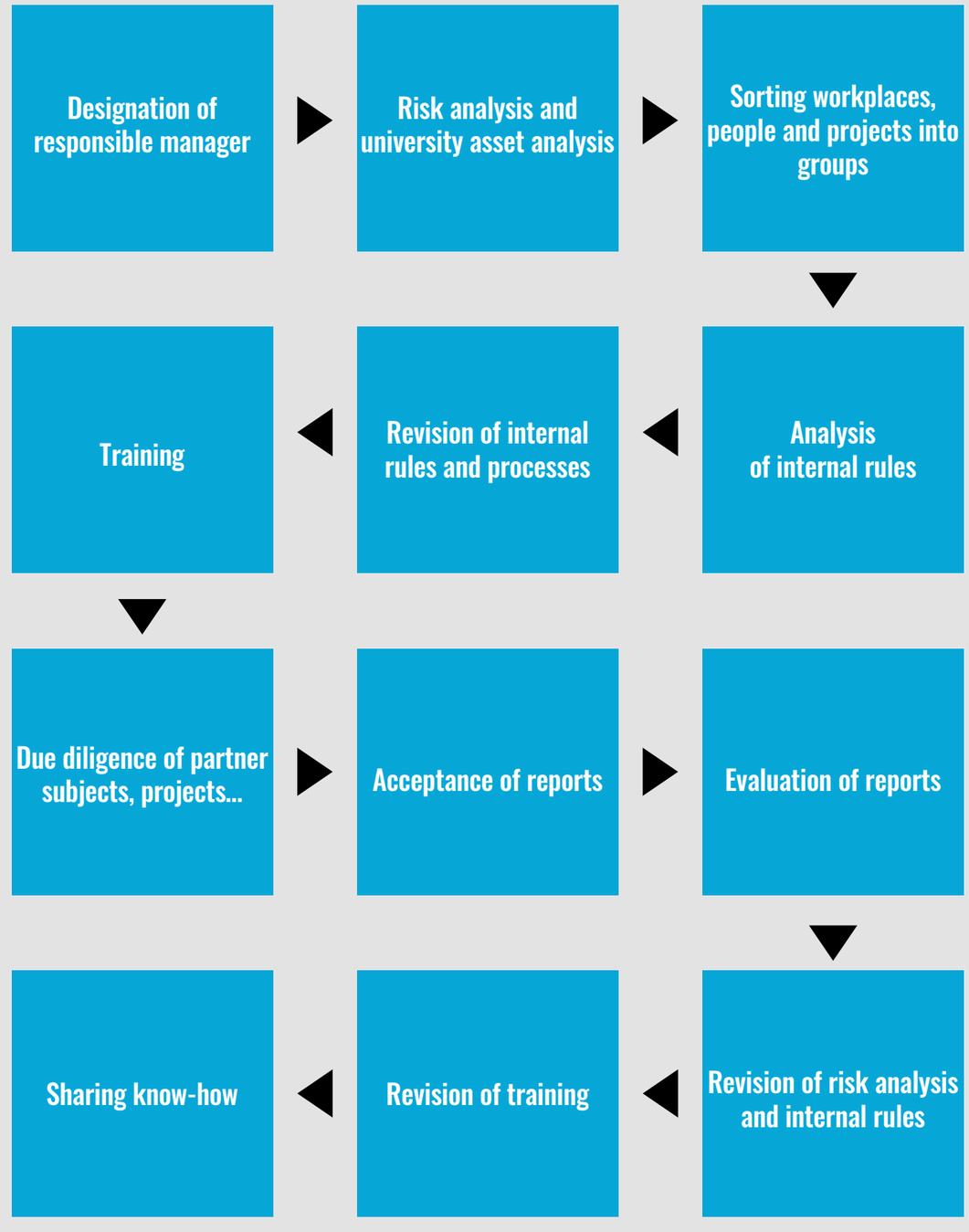
The National Office of Cyber and Information Security publishes a number of recommendations on its website[56,57] as well as methodic materials[58], training materials[59] and up-to-date information on various cybernetic threats[60].

The biggest weakness of IT systems is usually the people working with them. Therefore, it is necessary to train them properly to navigate the cyber world safely[61].

If a cybersecurity incident has already occurred, then the institution should have procedures in place to address such situations.

In the area of cybersecurity, similarly to other areas, setting clear and comprehensive rules seems to be an essential element of reducing the risk of interference. Equally important are timely responses to cyber security incidents, communication, sharing knowledge and experience, and training staff and students.

Simplified graphic representation of the process of setting up a system of protection against interference



5

Summary

The following steps can be recommended to increase resilience to interference in the higher education sector:

- Recognize that the risk of interference over HEIs and their employees is real.
- Identify a person at your institution who will be responsible for reducing the risk of interference.
- Include the risk of interference in your risk analysis and assess this for each level (top managers, staff identified as being at increased risk of interference, and other staff and students) as well as organisational unit and project (they face different levels of risk depending on what they do).
- Analyse existing safety rules and recommendations.
- Establish a strategy for reducing the interference; set up control mechanisms.
- Incorporate the “Know Your Partner” principle into your routine.
- Prepare a training system for staff and students.
- Conduct risk analyses repeatedly as the risk of interference might change over time.
- Follow the state’s or education authority’s regulatory requirements and adjust your internal rules against the interference accordingly.
- Create a registry of the institution’s financial income from foreign powers.
- Regularly evaluate the information you have on interference; use the findings and lessons learned to further improve your risk mitigation system.
- Prepare a communication plan in case of an incident including interference.
- Share your experience with other institutions.
- Establish clear rules for safe travel abroad, acceptance of gifts, conduct when dealing with foreign powers as well as for the political activities of students and staff.

6

Interference Techniques Focused on Individuals

The next part of the manual focuses on the most common interference techniques used by foreign powers. This is a demonstrative list, and we present each technique so that you can identify it if you encounter it personally. The section does not include all current and future techniques but selects the most commonly used ones. Just as threats and risks evolve, so do techniques for influencing individuals.

The following techniques of interference will be introduced: recruitment, elicitation, misuse of personal information from open sources, dangerous offers, risks while travelling abroad, blackmail and coercion.

6.1 Recruitment

Anyone can become an object of interest to a foreign power. It's just a matter of what the foreign power wants to achieve.

This technique[63] is one mostly used by intelligence services[64]. Intelligence services[65] use a variety of techniques to try to get people[66] they deem valuable to cooperate deliberately[67]. To do this, they very often choose to approach the person of interest directly through an intelligence officer, but they may also use intermediaries or various cover-ups. In the academic environment, attackers also often use various legitimate or seemingly legitimate entities to their advantage, such as scientific and technical libraries, scientific institutes and think tanks, organisations focused on expert exchanges or know-how transfer within the official exchange and talent programmes, consultancies, etc.

An intelligence officer may go under cover as a diplomat, businessman, researcher, student, etc. They may approach you under a "foreign flag" because they realize that cooperation or even just being in contact with someone from their country may be problematic for you.[68] If they pretend to be from a significantly less problematic country, you may be less wary and more interested in listening and cooperating.

It is also possible that you may find yourself in a situation where you are indebted to your attacker in some way – for example because they helped you in a moment of need or in a crisis situation.[69] The attacker can also get to you through your family or acquaintances, befriending them first.

Although often significantly less sophisticated, similar techniques are used by other entities to promote their interests. Many private entities also have enormous financial, technological and human resources at their disposal. They do not hesitate to use these techniques to their advantage to a greater or lesser extent, mainly to gain a competitive advantage and a stronger market position or to protect their interests. But how exactly do foreign powers go about recruiting people?

Attackers know what they want to achieve and look for ways to achieve it as efficiently as possible. Therefore, they begin by **guessing and gathering information** that could be used for the recruitment itself. The better the attacker knows their potential victim, the more advantages they will have in the later stages of the recruitment process. During the guessing process, attackers very often gather information that may, at first glance, appear to be worthless and non-threatening.[70]

Attackers are interested in finding out the relationship histories and minor transgressions of individual academics, people in managerial positions as well as others, in their property and familial relations, character traits, interests and hobbies, decision-making powers, in the preparation of public contracts and their tender documents, subsidy titles and grants, the composition of various committees deciding on tenders and in much more information of this sort.

When the attacker has sufficient information about their potential victim, they proceed to **make initial contact**. Most of the time, it is a short meeting; the sole purpose of it is to persuade the victim to meet up with them again. Sometimes the attacker approaches the victim directly. Other times they let someone the victim already knows introduce them as this increases the attacker's chances that the victim will agree to meet up with them again. In some situations, the attacker may put on a show to get the victim to approach them first and not the other way around. This is followed by **the friendship development phase**, where the attacker focuses on building a friendship with the victim. This always includes a pretend interest in the victim on the part of the attacker. The attacker may also take an interest in the victim's work and ask the victim to carry out an analysis or provide an opinion, insisting the victim uses publicly available information only. They pay their victim well for their work or provide them with other counter value. At some point, the attacker proceeds to the **recruitment** itself, which may be written, oral or implied. Gradually, the attacker starts requiring the victim to **disclose sensitive information**, and the victim is no longer able to say no because the only choice is to continue cooperating with the attacker or face employment penalties and possibly criminal penalties as well. However, these penalties cannot be avoided even if the victim carries on cooperating with the attacker.

In some cases, the foreign power takes a long-term approach and tries to enlist their victim early in their career.

Information gathering is a long-term activity. The attacker searches for people who have access to certain information or people who have access to the information they are looking for. It doesn't matter if you tell yourself that you are not important. If a potential attacker sees an attack on you as something that will help them reach their goal, then they will try. At the same time, **any institution is only as vulnerable as its weakest link**. Don't become a gateway through which an attacker can penetrate your institution.[71]

Anyone you meet outside your circle of trusted friends and colleagues can be working in the interests of a foreign power. This can never be reliably ruled out even with people you have known for a long time, since they may have started working for a foreign power after you met. In this case, pay attention to noticeable changes in behaviour and topics discussed especially.

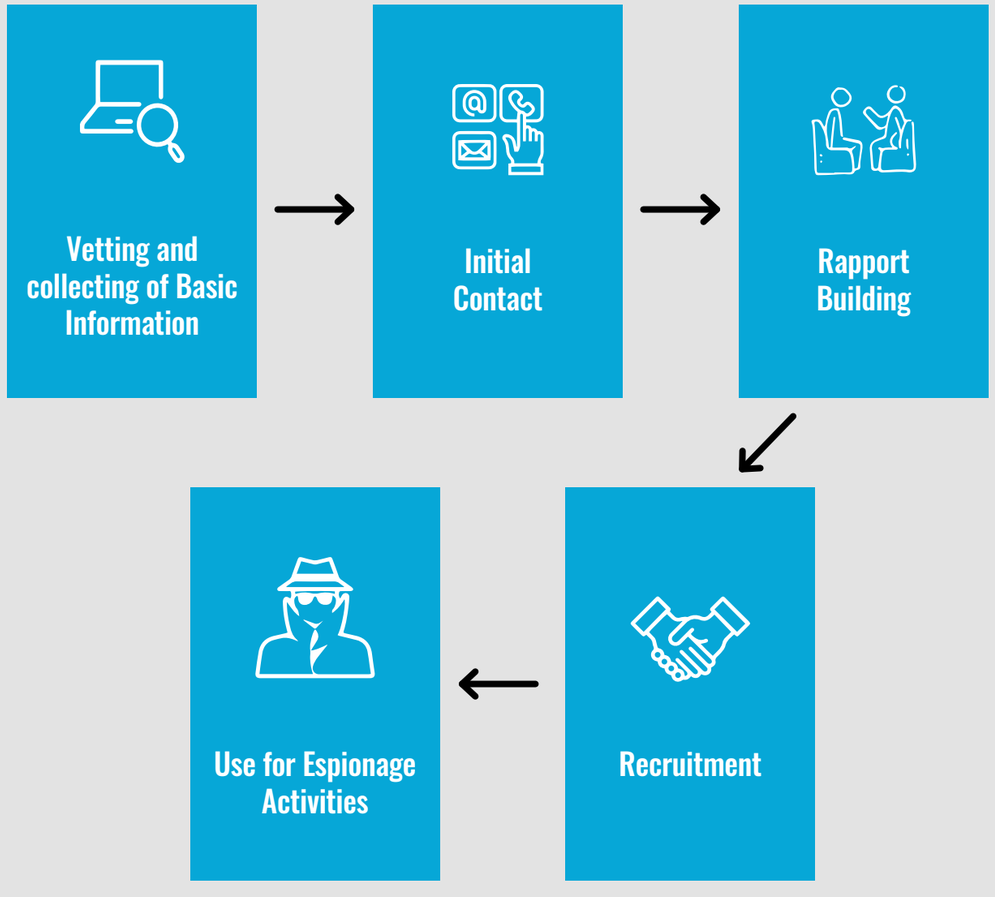
Take the time to think through:

- Which information about yourself and your work not to disclose or discuss only with your superiors, closest colleagues and family,
- Which information about yourself and your work to share and discuss only with your friends,
- Which information about yourself and your work to share with strangers,
- Topics to talk about when you get "stuck".

It may not be your fault at all if an attacker chooses you as the target of their activities. If you notice signs of an attempt at recruiting you, do not wait and contact your supervisor, security manager, the Czech Police or the Security Information Service. **Don't try to solve the situation all by yourself.** This could be a fundamental issue where your future life and career are concerned. Your level of decisiveness and the speed with which you proactively address the situation are extremely important. They can be what protects you from employment and/or criminal penalties.

To illustrate, the recruitment process can be visualized as follows:

Simplified recruitment process



72, 73

If you notice an attempt to recruit you by a representative of a foreign power, proceed as follows:

- Pay close attention to what the representative of the foreign power wants you to do.
- Remember as many details as possible (how you came into contact, who approached whom, who was the intermediary, what the attacker asked, what they were interested in, etc.).
- Ideally, respond to any offers for cooperation with a foreign power with a clear and distinct "no". That way your answer cannot be interpreted by the other party as a "maybe", "conditional yes" or "yes". Your clear and distinct negative response should discourage the other side from further attempts to recruit you.
- Don't say that you have to think things through, and don't joke. In such a case, the other party may interpret your response as a "maybe" or "conditional yes" and may very likely try to contact you again, using your first meeting to blackmail you.
- Inform the attacker that you will notify your supervisors and the security manager of the situation. This will discourage the attacker from further attempts to recruit you. It also tells the attacker that competent persons will learn abou their activities and consider adopting countermeasures.
- Inform your superiors and the security manager without delay. If you don't, the attacker will sense an opportunity to try to recruit you again. In addition, failure to inform your supervisor and security manager may later be held against you by your employer. It may jeopardize, for example, obtaining or renewing a security clearance from the National Security Agency or your employer if you apply for one.
- An exception to the procedure above for interacting with an attacker is when the attacker implicitly or explicitly threatens you. If you perceive a threat as real and you are legitimately afraid to confront the attacker and clearly refuse to cooperate, do not try to resolve the situation yourself. Instead, try to buy yourself time (even by pretending to take time to think). Then, without undue delay, inform your superiors and the security manager. If you are abroad, end your stay immediately and return home. Request assistance from the Czech security forces, ideally the Security Information Service, through the security manager. As professionals experienced in the situations described above, their representatives will then determine the next course of action.

Have you noticed any signs of a foreign power taking an interest in you? Trust your intuition. Don't wait to ask the professionals for help.

Possible signs of a recruitment attempt over social media

- You receive a message from a foreign university, research institute or company via a social network (most often LinkedIn, but also Facebook or Twitter and others).
- The profile that has contacted you is most likely to have a Western-sounding first name, but a surname that matches their country of origin. Very often it may contain a fake profile photo, sometimes generated by artificial intelligence, and an abstract and often semantically unclear description of the organisation on whose behalf the profile is contacting you. Very often, the organisation (or the person under the profile who contacted you) has no history, or does not even really exist. The text is likely to be written in poor English with many errors. The profile that has contacted you is likely to have quite a large number of connections and contacts, but these will usually suffer from similar flaws to the profile.
- You receive a request for advice or consultation (very innocent at first, usually within the scope of open sources). This is followed by an invitation for a working visit (in the country of "origin" of the profile) with all expenses paid by the inviting party.
- If you accept the offer, a meeting is set up with the person behind the profile which you were contacted from, which will most likely be attended by other colleagues of that person. A series of meetings similar to regular work meetings follows. Most of them take place in expensive hotels.
- You are asked to prepare an analytical assessment of trends in a certain area, to summarize publicly available and gradually also publicly unavailable and sensitive information (often of strategic and military use).
- You are offered an upfront payment for your work (usually in the form of cash, and usually more than one person from the inviting party is present). There is a high probability that a hidden recording will be made of the payment being handed over, with the aim of blackmailing you with it in the future.
- The inviting party starts requiring confidentiality of cooperation.
- Further communication is more likely to take place electronically (primarily through applications such as WeChat, Signal or WhatsApp, but also by e-mail). After some time, further face-to-face meetings are sought, ideally in the country of origin of the inviting party again. All travel expenses will again be covered by the inviting party.
- You grudually become fully involved in various espionage activities.

74, 75

6.2
Elicitation

Unconscious extraction[76,77] is one of the basic intelligence techniques. It is based on natural manipulation, which everyone uses to some extent in their everyday life. It is a way of getting as much information as possible from the target person without the target person realising they are giving any information away. It differs fundamentally from recruitment, which is an unambiguous offer of cooperation, meaning that in recruitment, there is usually no doubt about what is happening. The recruit has the option of saying "no".

A good manipulator who may try to exploit you will usually come across as a charming person. This is achieved using eye contact, compliments (in an attempt to give the impression that they think you are a capable and clever person), empathetic listening, occasional nodding, taking interest in what you say, and making you feel like their interests are close to yours. The use of this technique is not limited to face-to-face contact but can also be done to some extent over the phone or even in written form (emails, chat apps, text messages).

Why do unconscious extraction techniques work? Because attackers who use them are aware of the cultural and personality predispositions that people tend to have and they seek to exploit them.

The natural behaviors of humans as social beings that are most often targeted by attackers include:[78]

- Trying to be helpful and polite, even to complete strangers.
- Trying to look like someone who is very well informed.
- Seeking recognition and believing that one is contributing to something good.
- The tendency to talk about a topic if one gets a positive response.
- The tendency to spread rumors and gossip.
- Trying to correct others.
- The tendency to underestimate the value of the information communicated, especially in situations where one is unable to comprehensively evaluate how such information could be used.
- The tendency to believe that all people are essentially good and honest.
- The tendency to answer truthfully if one feels that a question was asked in good faith and with good intent.
- Trying to convince others of our one's personal truth.

The attacker usually contacts you seemingly at random or with a very plausible excuse. There may be multiple such "chance" encounters to reinforce trust. In academic environments, there are also situations where information is gathered using this technique by a person who is legitimately and officially present in your environment, such as an interpreter in a meeting with representatives of the other party or a contact person during a delegation visit to a partner institution. Using a prepared communication strategy, an attacker can gradually get a large amount of information out of you without you noticing anything suspicious. They create their own fictitious identity, a narrative, which is usually intended to stimulate your interest in further encounters with them. The attacker may initially talk to you mainly about themselves and seem uninterested in you. The aim is to manipulate you into a situation where you start giving up personal information or small things about your work.

The best defence against these techniques is a **healthy distrust and increased caution**. Be aware of what information you have that is sensitive or may be sensitive when placed in a broader context. Do not mention this information unless you have a very compelling reason to do so. Determine what information (about your work, family, etc.) you can share with anyone "in passing" and what is appropriate to share only with vetted and trusted individuals.[79]

The important thing to remember is that an attacker is never after your personal qualities but always after the information you have. Also, remember that you don't have to tell anyone anything at all. Do not, out of a sense of decency, allow yourself to be manipulated into a situation in which you become a victim of an attacker.

You can bring a conversation that you suspect is an attempt of elicitation back under your control in the following ways:[80]

- In your answers, refer to publicly available information (websites, newspaper articles, press releases…).
- Ignore questions or statements that you feel are inappropriate to the conversation and its content or try to change the topic of conversation.
- Respond to questions you perceive as inappropriate with a question of your own.
- Respond by saying "Why do you ask that?".
- Provide answers that are not completely specific.
- Do not be afraid to say, even if it is not true, that you do not have such information and simply do not know the answer.
- Declare that you will need to report the discussion to your supervisor and/or the security manager.
- Make it clear that you will not or must not discuss the given matter with the person.

6.3
Misuse of Personal Information from Open Sources

Approach posting information about yourself and your loved ones online with caution.

Attackers almost always make their first steps online.[81] They focus on what can be found about you from available websites. Social networks[82] (Facebook, Twitter, Instagram, LinkedIn, YouTube, TikTok, Twitch etc.) are an especially good source of personal information, e.g. where you go on holiday, which cafés you frequent, what your habits are, where you have studied, where you work and live or where you come from.[83] Social media display at least some of the relationships between the people you meet, and this does not apply solely to your friends' list, but also to the photos and videos posted not only on your profile but also on the profiles of dozens (and maybe hundreds) of your friends and family. By analyzing the visual information and visible messages and comments that are accessible, it is often possible to gain a basic overview that can be used by an attacker to seek additional insights.

Social networks themselves store a huge amount of information about users and their habits. Their business model is based on selling much of this information in anonymised form to other entities that advertise with them. Users agree to this practice by confirming the terms and conditions when creating an account. Social networks and their operators usually collect information about their users not only from the information directly provided to them by the user (e.g. when they create an account) but also from information that is directly and indirectly derived from the user's behaviour on the social network. This information includes their place of residence, age, gender, marital status, information on a recent move, pregnancy, the age of their car, donations to charities, gaming, use of debit cards, shopped-for groceries, income, property ownership and value, long-distance relationships, work environment, browser gaming, use of game consoles, interest in purchasing cosmetics, preferred type of restaurants, interest in sporting events, and much more.[84]

On social networks, attackers can search very easily according to predetermined criteria. It is also possible to compare two different profiles – what the people in question have in common and their connections. Information can be searched using a person's employer, place of residence, religion, etc. There have also been large-scale leaks and misuse of social network users' personal data.[85]

Other publicly accessible information can be found in some state institutions' databases, such as the Trade Register, the Register of Business Entities, the Land Registry, lists of university students – this is information that is entered into these databases without your consent. The above is not an exhaustive list of possible sources that can be searched. There are also, for example, news media and their archives, blogs, personal websites, various quasi-media servers, and even internet archiving services.

Attackers often try social engineering methods and may call or send you a message via social networks, email or text message. What makes it easier for the attacker is that at least some of your contact information is public by nature because of your work in the higher education sector.

However, attackers can also wiretap your phone, office or home. You may also be tracked in order for the attacker to find out more about your life, habits and contacts. Phone, office or home tapping or surveillance has long been the domain of security forces. There are a number of private entities that specialize in these activities that can be hired.

Some basic tips to improve your online security

Generally

- Check what private information of yours is available on social media. Remove unnecessary information.
- Set the security of your social media accounts so that their content is only visible to your circle of friends.
- If you are working on a sensitive project, do not disclose this information.
- Try not to let your economic situation be known. Do not disclose your salary (wages). Do not publish photos of your house, apartment, etc.
- Before you travel abroad, make sure you double-check what personal information of yours can be publicly tracked on social media.

Abroad

- Do not log into private or work emails, your Google (Microsoft/Apple) account, social networks or internet banking. If you must do so, use a VPN connection.
- Do not connect your devices (mobile phone, laptop, tablet and such.) to Wi-Fi networks in public places, railway stations, airports, hotels or cafés.
- Do not use your personal or work phones, laptops or various data carriers (USB, external HDD, etc.) and if possible, use prepaid SIM cards and mobile phones that you do not intend to use again in the future. Ideally, use a borrowed laptop and have it reinstalled when you return.
- Do not use data carriers or any electronic devices you have received as a gift or found somewhere.

88, 89, 90

6.4 Dangerous Offers (Invitations to Events, Gifts, Paid-for Training, Paid-for Travel)

Various social events, conferences, seminars or formal and informal business meetings may be places where you face unconscious extraction of information or attempts at recruitment.[91] **Many of these events are organised for this very purpose.** They can be used to get to know you and to make initial contact, which may seem very innocent at first. The programme of your stay and on-site activities may be blown up on purpose to reduce your vigilance and, consequently, your full control over what information you give.

It is also an opportunity to give out various small gifts to those present.[92] **Especially gifts in the form of data carriers (especially various CDs, DVDs or USBs) may contain a spyware** that is activated the moment the user plugs the data carrier into the computer.[93] In most cases, spyware is so sophisticated that even antivirus scanning is unable to detect it. An infected computer will allow sensitive information to be sent to the attacker's computer. The spyware can also attack your institution's entire computer network. Even if a gifted device is used exclusively at home, the recipient and their entire family are at risk of their useful personal, contact or even compromising information being collected. Your home computer can then be taken over by an attacker and used to attack the computer networks of your college, as well as those of other entities with which your college works.[94]

Beware of gifted data carriers. Do not insert or connect them to your computer at work or at home. Do not open unsolicited emails.

Attachments to emails and messages sent via communication apps such as WhatsApp, Viber, Signal and others carry similar risks as data carriers. This is especially the case if such an attachment, document or website link has been sent to you by an unknown person. You should also be cautious if the message is from a colleague or friend, especially if you are not expecting such a message. In such cases, it is better to check with the person in person or by phone to make sure they sent you the message in question. If you have suspicions that malware may have gotten onto your computer, contact your IT department (network administrator) and shut down your computer to prevent the further spread of the malware.[95]

6.5
Risks While Travelling Abroad

Prepare carefully and be cautious when travelling abroad.

Travel and contacts with foreign countries are part of the academic sector, whether it be a study visit, an internship, a trip to an international conference or participation in the Erasmus or another exchange programme.[96] The risks of academic staff as well as students being influenced on foreign business and private trips are very real.[97, 98] Your attention is focused on realizing the goal of your journey. However, it opens up space for the attacker to approach you, knowing that if things don't go quite as they want, you are less likely to report your suspicions or discuss them with someone immediately.

Your mobile phone, computer, data carrier and even your notes can be copied during a border check or other, even staged, police check. On these occasions, an attacker can also install spyware on your computer. **You should never leave technology and data carriers unattended elsewhere, either** – in a hotel room, at a reception or restaurant, but also during meetings, conferences, etc. Similarly, dangerous situations arise if you use shared mobile phone chargers and publicly accessible Wi-Fi networks.[99] Both are very often exploited to install malware[100] to connected devices or to steal the data stored on these devices.[101] Similarly, do not take cards or chips used as a key for various electronic access control systems with you when travelling abroad. These can also be taken, copied and later used to attack your workplace. The same applies to the various cards, chips and tokens that you use to authorise your login to the computer network or as your electronic signature.

Also pay increased attention to situations where an exceptional opportunity arises during your trip or stay abroad[102] to meet someone very important, be it a local executive, a businessperson who is interested in your research and offers to monetise the results well and profitably for you, or another important person. Particularly if they are individuals with ties to undemocratic and illiberal states and regimes or with ties to various corporate entities as well as various innovative companies or firms looking for new talent and investment opportunities, there is a serious risk that they are actually trying to get you to cooperate with them.

Documents containing sensitive or exploitable information, as well as technology, should be kept with you at all times or not taken abroad at all. This can be supporting material, but it can also be a notebook with your thoughts, observations, or contacts. Always keep such documents where you can see them or in your hand luggage, do not leave them in your hotel room and do not put them in your checked luggage when travelling by plane.

Visits by representatives of a foreign power to your workplace can also pose a risk. The delegation may include a person tasked with obtaining sensitive information. This does not have to be a foreign visit. A foreign power may also attempt to probe for sensitive information through persons who introduce themselves to you as students, journalists, representatives of academia or non-profit organizations, etc.

46

Possible signs that you have been targeted by a foreign power at a border/police check

- The verification of the documents you submitted (and other documents) takes an unusually long time.
- You are escorted to an interrogation room or police station for no apparent reason.
- Without any introduction, a plain-clothes officer appears and starts asking you a series of questions unrelated to the reason for the initial check; the plain-clothes officer is likely to not be alone, with at least one other plain-clothes officer appearing in the course of the conversation, keeping quiet but listening carefully and asking follow-up questions.
- You are asked about your exact job title and the details of your work, but also about your contacts; you may be asked to give up your contacts' addresses and phone numbers, emails, etc., as well as information on whether they travel, how often, and to which countries.
- If you refuse to answer questions, it may be implied that you have violated local laws; sometimes even including a specific illegal act (whether existing or fabricated).
- You are given two choices: Either you accept to start cooperating with the local intelligence service or you will be banned from entering the country for life, and your current visa will be revoked. If you refuse to cooperate, you may even be threatened with imprisonment.
- The officer who interviewed you gives you their phone number, email or another way to contact them next time (and to report, for example, your next trip to the country or abroad in general).
- You are informed that you are not to deny or otherwise sabotage the cooperation, and they advise maintaining confidentiality about your conversation and mutual agreement.

103

47

6.6
Blackmail and Coercion

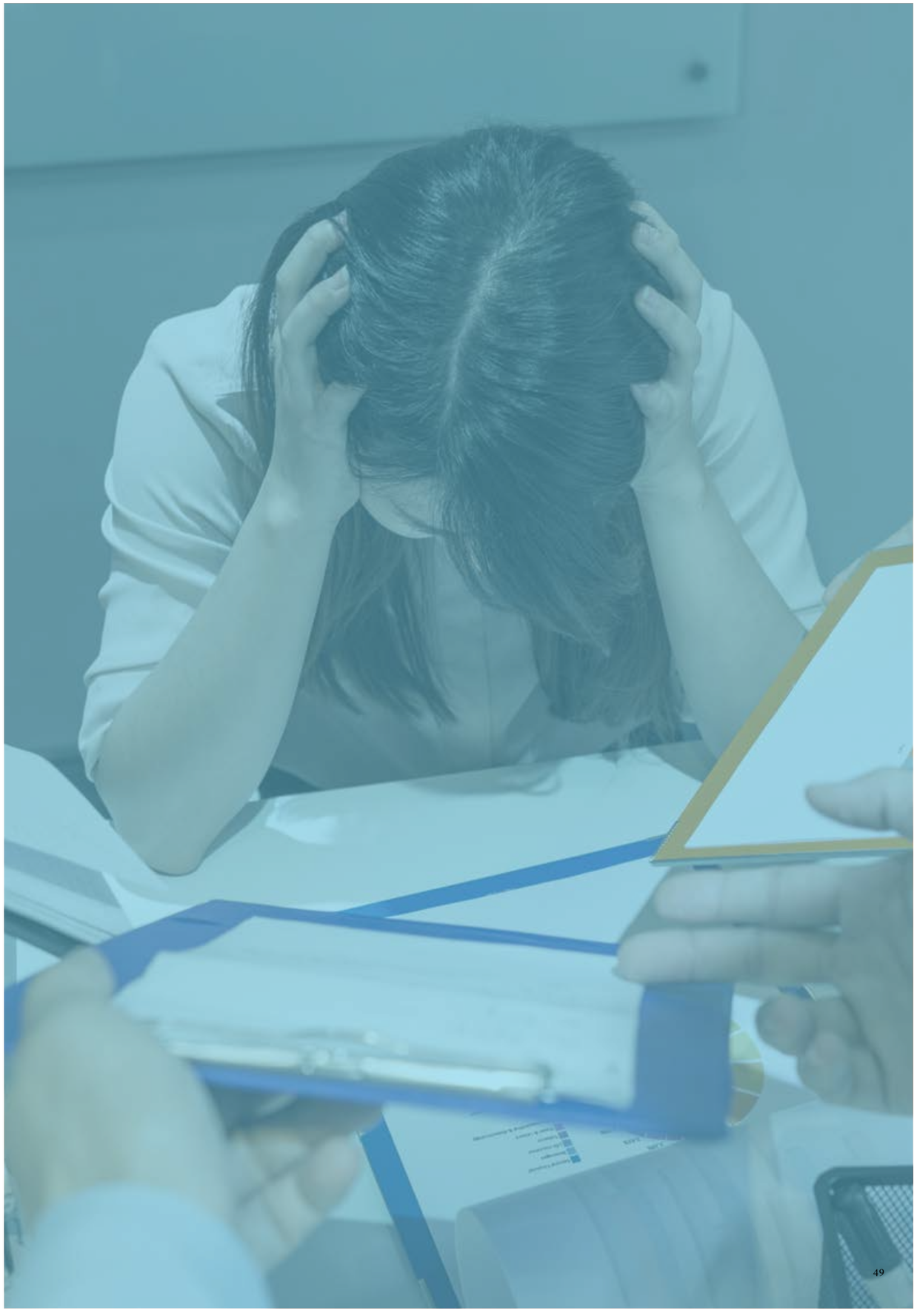
Don't deal with blackmail alone; confide in someone.

It is still a very frequently used technique, although it may seem to belong to spy films only. In particular, foreign powers that do not feel bound by the rule of law and fundamental human rights and freedoms will are unlikely to be reluctant to use blackmail and coercion. Therefore, try to limit the risk of finding yourself in a situation where you could be blackmailed as much as possible.

Be aware that your trips abroad, in particular, can put you in a situation like that. It may not be your fault or mistake, but a scenario carefully plotted in advance by the attacker. However, any secret can be misused if you are genuinely concerned about it becoming public knowledge. There can be many such things, from alcohol, betting or gambling to sexual adventures and various regressions, including those of the past. But in the end, it could be anything you want to keep secret from those around you.[105]

The attacker will use all the power and means at their disposal that allow them to obtain blackmail material against you. In places open to the public, they will try to follow you and take photographs, videos or audio recordings of compromising situations you get into, either yourself or as part of a prepared scenario. They will try to take control of the technical and communication devices you use at home or at work and make a record of potentially compromising activities. If that proves insufficient, they will try to install a spy device (called a "bug") in your home or work. If the attacker cannot obtain a compromising recording naturally, they will try to manipulate you into a potentially compromising situation. Thanks to the technically advanced software we have today, they may also use photo and video editing (and create a so-called deep-fake video) to fake the compromising material. They can find a person to accuse you of something and file a criminal complaint against you. They can run a smear campaign against you on the internet. All of this is done to force you to cooperate or to discredit you for refusing to cooperate.

If you notice an attempt to coerce or blackmail you, **do not deal with the situation alone. Confide in your family and contact the security manager** at your university or faculty. You can also contact the Czech Embassy abroad. Although you may feel that the help you get this route is not what you would have imagined, you will get several important things. Sharing your situation with an uninvolved person and discussing it with them will help you to put things into perspective; you will be able to think the situation through, and, most importantly, you will have a witness who will testify that you tried to resolve the situation promptly, which may be essential for your future credibility. Ultimately, however impasse the situation may seem, succumbing to blackmail and coercion always results in consequences far worse than when openly dealing with the situation with the help of responsible persons and authorities.



7

What Are You at Risk Of?

Don’t risk your professional and private life.

The most serious risks to you as an individual include loss of professional prestige, loss of employment (dismissal from employment for breach of employment obligations under the Labour Code, exclusion from a research project or grant) and subsequent family and personal difficulties, which can take many different definitional forms. You may also face criminal prosecution in connection with your work for a foreign power. You can find a large number of cases in the open sources where cooperation with a foreign power turned out badly for the cooperator. **Do not risk your professional and private life for a short-term gain or relief**, even in situations that you perceive as hopeless at the time. In the vast majority of cases, succumbing to the pressure of a foreign power ends far worse than dealing with the situation the standard way.

The main principle to remember is **“If you see (perceive) something, then say something”**.[106] This is in no way about building a “snitch” culture in the higher education sector. However, it is necessary to reflect that every employee in the higher education sector is part of the puzzle that ultimately helps keep the academic environment free, democratic and creative, and thus defends universities against unwanted influence from outside powers. Both transparency and precaution are essential in these cases. **It is always better if your security manager or supervisor assesses your report as unfounded and concludes that there is no foreign influence than to downplay the situation, pretend that nothing is happening, and face far worse consequences.**

Although even after a system is in place to identify and manage the risk of foreign influence, one or more individuals at your institution may fail – because **where there are people, there are human weaknesses – therefore the preparedness of all involved is critical in this area.**

Through your responsible approach, your unviersity will become more resilient and better able to respond to situations where the risk of foreign influence is present, which will also reduce the potential negative impact of such a situation.

8

Final Summary of the Interference Techniques on Individuals

Have you become a target of interest to a foreign power? Possible warning signs include:

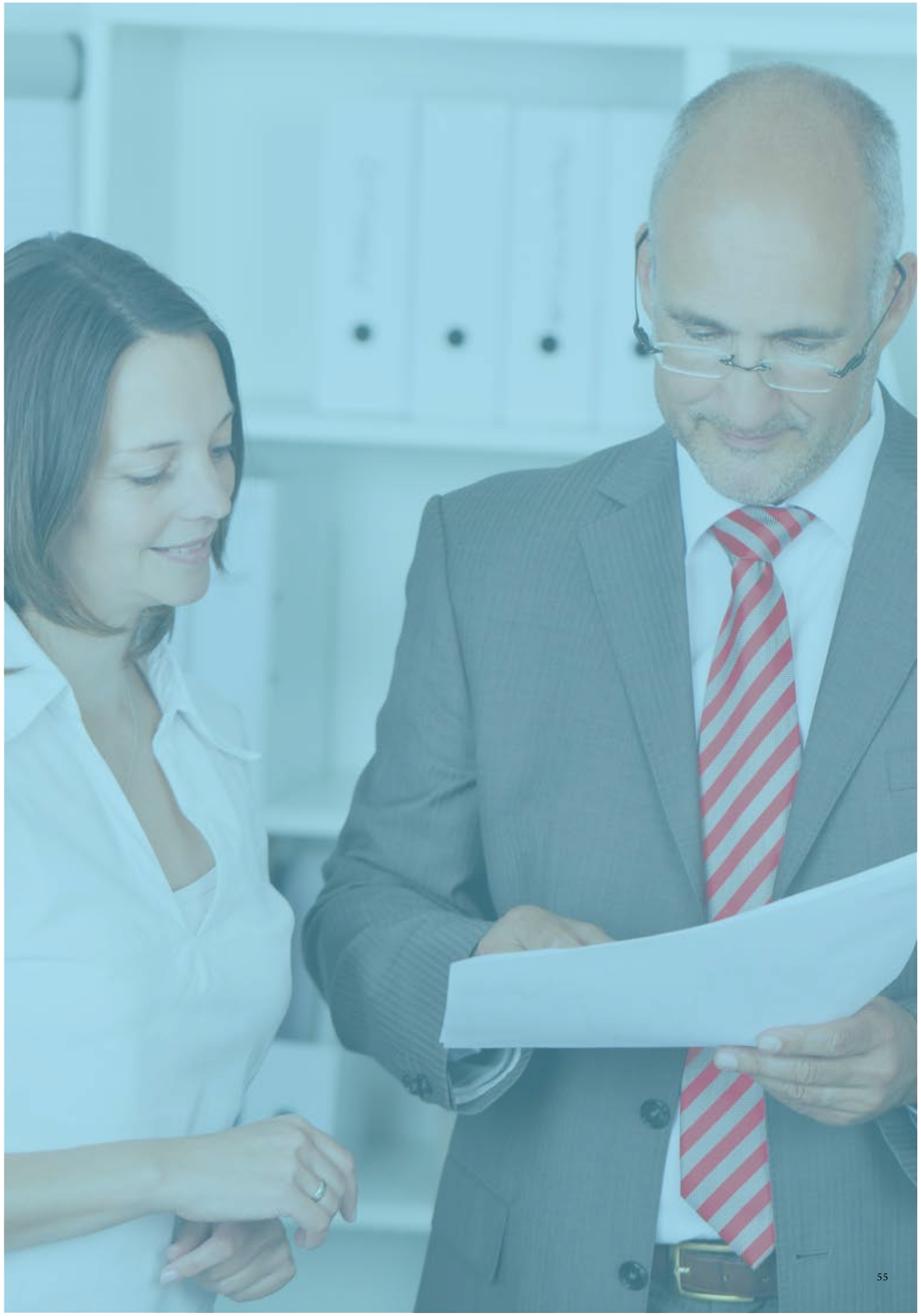
- A new, interested acquaintance appears, asks more questions than is standard about your work, hobbies and life, shows exceptional knowledge about your work or life. Beware that your long-time acquaintances or friends can be used to gain information about you for a foreign power if they have begun cooperating with a foreign power.
- You get unexpected advantageous job offers from a foreign institution or company.
- You receive requests for documents that can be obtained elsewhere.
- On your travels, you find signs of your personal belongings, luggage, electronics, etc. being tampered with.
- You encounter attempts to suddenly separate you from your belongings, phone, laptop, etc.
- You get a sudden offer to meet a high-ranking or otherwise highly respected person.
- You unexpectedly meet a former colleague who started working abroad.
- A possible sign that information from your workplace is being obtained by a foreign power is when your work partner shows more knowledge of the subject matter than they should have.

Be aware of the basic principles of defence against foreign influence:

- Everyone can be interesting to a foreign power – even you.
- Any information can be very interesting to a foreign power. Even the seemingly most trivial information can be misused.
- Anyone you meet outside your circle of trusted friends and colleagues can work in the interest of a foreign power. This can never be ruled out even with people you have known for a long time because it is possible for them to have started working for a foreign power only after you met. In this case, pay attention to any noticable changes in behaviour and topisc discussed.
- Make sure that information available about you online and elsewhere corresponds to the categories defined above, and follow this rule in your communication (email, phone, letters etc.)
- If you think that you have found yourself in an unusual situation or that you have become the target of a recruitment attempt, do not panic and inform the relevant contact person. The longer you cooperate with a foreign power, the worse it can get.

General recommendations to conclude:

- Be aware of suspicious activity towards youself as well as situations where you believe you may be the target of solicitation or recruitment or when you experience unusual interest in from others.
- If you think something is wrong, do not try to resolve the situation yourself. Create records and reports and share these with the security manager at your university. Do not be affraid to ask for advice. You can contact your supervisor, the security manager of your university or faculty, or, if warranted, the Security Information Service directly.
- We advise you to exercise extra caution when it comes to offers of foreign business trips or invitations to internships and conferences, especially if they are not necessary for your work performance. Be particularly careful if the organizer offers to cover your expenses and give you allowance.
- When travelling abroad for work, don't let yourself be manipulated into a compromising situation (alcohol, company at the hotel room etc.). Keep your documents, laptop, mobile phone or USB with your personal information with you at all times, do not leave them in the hotel room safe (the hotel management has a master code in case guests forget the access codes and cannot get into the safe to retrieve their valuables). When travelling to and from your trip abroad, don't leave these items in luggage that you don't have in sight at all times.
- If you are accompanying foreign visitors to your workplace, keep track of where the visitors are, do not allow them to move freely around the building and do not leave them alone in your office or the offices of your colleagues.
- Before travelling abroad, consider whether you need to bring your own technology such as a laptop and phone. Leaving them at work or at home reduces the risk of losing your information or infecting your technology with harmful software.
- If you need to connect to the internet, please note that your communication may be monitored in various places (cafés, hotel, airport, etc.). Your internet provider can always view what you are doing online. Use a VPN.
- If possible, avoid using public Wi-Fi networks, hotel computers and internet cafés – those are generally not very secure.
- Share only the necessary information on social media and in emails and set your privacy as high as possible. Check these settings repeatedly.
- Approach various courtesy gifts in the form of flash drives, memory cards, etc., with the utmost caution as they may be infected with harmful software. Keep in mind that you can also infect your computer by visiting various websites and always consider whether they are trustworthy. Constantly update your operating system and all security applications (antivirus software, firewall).



9

Contacts

Methodological questions

Centre Against Terrorism and Hybrid Threats
Department of Secuty Policy
Ministry of the Interior of the Czech Republic

Email: cthh@mvcr.cz
Website: www.mvcr.cz/cthh/

Incident Reporting:

Security Information Service
Email: prevence@bis.cz and info@bis.cz
Website: www.bis.cz

Police of the Czech Republic

Website: www.policie.cz/imapa.aspx

10

References

[1] https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788

[3] http://www.europarl.europa.eu/RegData/etudes/ATAG/2019/644207/EPRS_ATA(2019)644207_EN.pdf

[4] https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1564018 & t=e & l=en

[5] https://www.cdse.edu/index.html

[6] https://publications.parliament.uk/pa/cm201919/cmselect/cmfaff/109/10902.htm

[7] https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Pages/managing-risks-in-internationalisation.aspx

[8] https://www.hrk.de/positionen/beschluss/detail/leitfragen-zur-hochschulkooperation-mit-der-volksrepublik-china/

[9] https://docs.education.gov.au/system/files/doc/other/ed19-0222_-_int_-_ufit_guidelines_acc.pdf

[10] https://www.research.uky.edu/office-sponsored-projects-administration/guidance-regarding-foreign-influence-university-research

[11] https://www.research.uky.edu/office-sponsored-projects-administration/guidance-regarding-foreign-influence-university-research

[12] https://www.ucop.edu/ethics-compliance-audit-services/compliance/research-compliance/foreign-influence.html

[13] https://researchservices.cornell.edu/policies/guidelines-on-undue-foreign-influence

[14] https://research.unl.edu/researchcompliance/foreign-influence-international-activities/

[15] Sometimes called a "soft power".

[16] The Australian think-tank Lowy Institute has been the target of at least two hacker attacks aimed at stealing the database of contacts of people with whom the think-tank cooperates and who attend events organised by the think-tank. Moreover, other Australian and American think tanks have faced similar hacking attacks. (https://www.smh.com.au/national/watering-hole-attacks-how-china-s-hackers-went-after-think-tanks-and-universities-20181203-p50jxj.html).

[17] Aston University in Birmingham, UK, investigated complaints from Hong Kong students that their Chinese classmates harassed them. Mainland Chinese students surrounded a student supporting the democratic process in Hong Kong so that he was unable to leave while the Chinese students standing around him held a Chinese flag and sang the national anthem. Other Hong Kong students fear that fellow mainland Chinese students are monitoring them, identifying their social media accounts and sending their photos to China. (https://www.telegraph.co.uk/news/2019/10/12/police-called-hong-kong-china-tensions-spread-uk-universities/).

[18] In February 2020, Germany's Trier University faced a wave of criticism for academic philosopher Andreas Lammer accepting the World Award for Book of the Year of the Islamic Republic of Iran. This was awarded to him by Iranian President Rouhani for his work focusing on Islamic scholar Ibn Sīnā, who died in Hamedan (present-day Iran) in 1037. The criticism stemmed mainly from Iran's human rights violations and support for terrorism, which should be reason enough for not accepting or rejecting the award. (https://www.jpost.com/Diaspora/Antisemitism/German-university-under-fire-for-accepting-award-from-Irans-regime-617996).

[19] In January 2020, the collaboration of Professor Gu Jian, a professor at China's Hainan University working on information security, with China's Ministry of State Security (MSS) was uncovered. He used his position to recruit young IT professionals to work for the APT40 hacker group controlled by the Hainan headquarters of the MSS. Gradually, 13 companies were uncovered that very likely acted as front companies for APT40 and were allowed by Professor Gu Jian to post job advertisements on the Hainan University website. (https://intrusiontruth.wordpress.com/2020/01/14/who-is-mr-ding/, https://intrusiontruth.wordpress.com/2020/01/16/apt40-is-run-by-the-hainan-department-of-the-chinese-ministry-of-state-security/, https://intrusiontruth.wordpress.com/2020/01/10/who-is-mr-gu/, https://intrusiontruth.wordpress.com/2020/01/13/who-else-works-for-this-cover-company-network/).

[20] For academic freedoms, see Section 4 of Act No. 111/1998 Coll., on Higher Education Institutions.

[21] Four academics working at UK's London School of Economics (LSE) objected in front ot LSE's chancellor in June 2019 to the "increasing reputational risk to the school for its intensive collaboration with China" and demanded "a careful review of the ethical implications of having shared teaching and research programmes at the LSE with institutions where the Chinese Communist Party is curtailing academic freedoms" (https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all-1573-rdf).

[22] Universities in the U.S. and elsewhere in the world have become aware of the controversy surrounding Confucius Institutes. These institutes were founded to promote the study of Chinese language and culture, but many academics currently see them as a front for Chinese intelligence services (https://www.voanews.com/student-union/chinese-college-students-being-forced-spy-us).

[23] In 2019, the UK's London School of Economics was forced to suspend a planned programme of collaboration with Shanghai businessman Mr Li, which promised generous research funding and a share of funding for teaching within Masters and PhD programmes on Chinese economics, politics and society, with a panel of eminent Chinese figures to oversee the accuracy of the content (https://www.ft.com/content/2dd5ed50-f538-11e9-a79c-bc9acae3b654).

[24] https://www.dailymail.co.uk/news/article-8535623/How-Britain-teaches-China-conquer-West-UKs-universities-share-research-China.html

[25] In April 2019, U.S. FBI Director Christopher Wray warned that Chinese intelligence agencies are pushing hard on Chinese students studying in the U.S. and their families in China to "bring home" valuable intellectual property, or the families will fare poorly (https://www.voanews.com/student-union/chinese-college-students-being-forced-spy-us).

[26] Britain's London School of Economics (LSE) faced widespread public criticism in February 2020 for considering a three-year consultancy contract with Chinese firm Huawei, whereby it was to research the firm's "leading role in the development of 5G technology" (https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all- -1573-rdf).

[27] https://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/kontrola_exportu_zbrani/mezinarodni_spoluprace/mezinarodni_kontrolni_rezimy_obecna.html

[28] https://www.mpo.cz/cz/zahranicni-obchod/licencni-sprava/

[29] https://www.financnianalytickyurad.cz/

[30] https://occrp.org/en

[31] www.hsgac.senate.gov/imo/media/doc/PSI%20Report%20China%27s%20Impact%20on%20the%20US%20Education%20System.pdf?utm_content=&utm_medium=email & utm_name=&utm_source=govdelivery & utm_term=

[32] https://www.aspi.org.au/report/party-speaks-you

[33] https://unitracker.aspi.org.au/

[34] https://www.aspi.org.au/report/picking-flowers-making-honey

[35] In October 2019, the Rector of the Charles University in Prague signed a partnership agreement with a loaning firm Home Credit. This move provoked a strong reaction from some academics, students and the public. Within a few days, in response to an extensive public debate criticising the partnership, Home Credit withdrew from the contract. (https://www.seznamzpravy.cz/clanek/konec-kritiky-na-akademicke-pude-odbornici-jsou-proti-partnerstvi-univerzity-karlovy-s-home-creditem-80303, https://www.seznamzpravy.cz/clanek/home-credit-po-vlne-kritiky-vypovedel-smlouvu-s-karlovou-univerzitou-80463, https://www.respekt.cz/tydenik/2019/42/univerzita-kellnerova).

[36] In 2011, a scandal broke out at UK's London School of Economics (LSE) over the receipt of funds from a foundation run by Saif Al-Islam, the son of the then Libyan dictator Muammar Gaddafi, and there were strong suspicions that the funds may have come from bribes. The affair eventually ended with the resignation of the LSE Rector. One of LSE's subsidiaries also won a contract to train Libyan civil servants, which also inspired a wave of disapproval and criticism (https://www.theguardian.com/education/2011/nov/30/gaddafi-donation-lse-bribes-inquiry, https://www.ft.com/content/2dd5ed50-f538-11e9-a79c-bc9acae3b654, https://www.dw.com/en/is-londons-lse-helping-huawei-clean-its-reputation/a-52425672?maca=en-rss-en-all-1573-rdf).

[37] At the end of 2018, the US began investigating some American universities for their funding by Qatar as well as other Middle Eastern states. By providing generous financial contributions, Qatar was primarily pursuing its foreign policy objectives, and thus abusing US universities. Moreover, much of the financial flows lacked transparency and were kept secret from the US authorities by the US universities (http://english.alarabiya.net/en/features/2018/12/20/How-Qatar-is-paying-1-3-billion-to-US-institutions-to-gain-dubious-influence.html, https://clarionproject.org/exclusive-foreign-funding-billion-dollar-black-hole/, https://www.novinky.cz/zahranicni/amerika/clanek/bernak-jde-i-po-harvardu-a-yale-40313470?seq-no=5 & dop-ab-variant=&source=article-detail).

[38] https://gacr.cz

[39] https://tacr.cz

[40] See Act No. 2/1969 Coll., the Competence Act (https://www.zakonyprolidi.cz/cs/1969-2).

[41] In October 2019, information was published indicating that the Centre for Security Policy at the Faculty of Social Sciences of Charles University, led by PhDr. Balabán, had carried out several not-quite-standard actions that it was unable to explain clearly and transparently (e.g. There was a private company of the same name, which received some of the funds that were supposed to go into the accounts of Charles University; some of this money also came from the embassy of the People's Republic of China; PhDr. Balabán also taught a course on China at the Faculty of Science of Charles University, which was financed by the Chinese embassy, etc.). In response to this situation, the employment contract of PhDr. Balabán and his other two colleagues from the Centre for Security Policy with the Faculty of Social Sciences of Charles University was terminated. CU estimates the amount of financial damages alone at around five million crowns (https://zpravy.aktualne.cz/domaci/univerzita-karlova-vazby-milos-ba- laban/r~5dc6cc54017811eab259ac1f6b220ee8/, https://www.respekt.cz/politika/za-odmenu-s-karlovou-univerzitou-zdar- ma-do-ciny, https://echo24.cz/a/Sifk9/horka-puda-na-univerzite-konflikt-mezi-akademiky-miri-k-eticke-komisi, https:// archive.ihned.cz/c1-66722060-police-investigating-million-damages-at-karlov-university?utm_source=mediafed & utm_media=rss & utm_campaign=mediafed).

[42] The Massachusetts Institute of Technology (MIT) has repeatedly accepted millions of dollars from the Saudi government despite protests in the academic community over the donor's impropriety. The protesters were particularly concerned about human rights violations by the Saudi government. In October 2018, following the murder of journalist and opponent of the Saudi government Jamal Khashoggi, MIT was forced to return the unspent money under public pressure and faced widespread public criticism for accepting donations from such problematic donors (https://www.nytimes.com/2019/07/03/magazine/saudi-arabia-american-universities.html).

[43] In August 2018, information was published that the Iranian hacking group Cobalt Dickens attacked 76 universities in 14 different states with the aim of violating intellectual property protection and stealing intellectual property (https://www.independent.co.uk/life-style/gadgets-and-tech/news/iran-hackers-uk-university-cyber-attack-security-cobalt-dickens-a8506406.html).

[44] https://www.zakonyprolidi.cz/cs/2004-594

[45] An investigation by the UK security services has found that some 500 Chinese scientists currently involved in Chinese military research have studied at British universities in the last ten years alone, including in areas such as technologies used to build fighter aircraft, supercomputers and ballistic missiles (https://www.thetimes.co.uk/article/security-services-fe- ar-the-march-on-universities-of-beijings-spies-gv9pk3hzr).

[46] In July 2017, Chinese-American student Si Yue-Wang from Princeton University was sentenced to ten years in prison for spying for the U.S. while studying in Iran. Si Yue-Wang specialized in the late 19th and early 20th century as part of his doctoral studies and travelled to Iran to research the Qajar royal dynasty. Thus, the most likely reason for the student's imprisonment was Iran's desire to obtain hostages to exchange for its citizens imprisoned in the U.S. Two years later, in December 2019, the U.S. and Iran finally swapped their prisoners, and Si Yue-Wang was set free (https://domaci.ihned.cz/c1-65801730-v-iranu-odsoudili-na-deset-let-americkeho-studenta-za-udajnou-spionaz-maskoval-ji-pry-vedeckou-praci, https://ct24.ceskatelevize.cz/svet/2998580-vedce-za-studenta-americane-a-iranci-si-ve-svycarsku-vymenili-vezne).

[47] E.g. Princeton University travel advice (https://informationsecurity.princeton.edu/intltravel).

[48] Latvian State Security Service, Annual Report 2019 (p. 23, https://vdd.gov.lv/en/?rt=documents & ac=download & id=55).

[49] In autumn 2019, riots broke out at the University of Sheffield in the UK between students from Hong Kong and Taiwan on the one hand and students from mainland China on the other. An elected representative of international students hailing from China urged other Chinese students to report Hong Kong and Taiwanese students to Chinese security forces (https://thetab.com/uk/sheffield/2020/02/12/sheffield-university-hong-kong-chinese-students-sissi-li-42125).

[50] E.g. The Swedish manual for communicators available in Czech and English on CTHH website (https://www.mvcr.cz/cthh/clanek/boj-proti-informacnim-vlivovym-aktivitam-prirucka-pro-komunikatory.aspx; https://www.msb.se/RibData/Filer/pdf/28698.pdf).

[51] For more details, see e.g. the Communication section (pages 29-32) of soft target coordination methodologies for the post-security incident phase (in Czech). (https://www.mvcr.cz/cthh/soubor/metodika-koordinace-mekkeho-cile-pro-fazi-po-bezpecnostnim-incidentu-aneb-jak-se-vyrovnat-s-nastalou-situaci-g-ben-david.aspx).

[52] https://www.policie.cz/imapa.aspx

[53] https://www.bis.cz/kontakty/

[54] In March 2018, the U.S. Department of Justice charged nine Iranians with large-scale data theft. Among those behind the robbery was Mabna Institute, an Iranian firm working with the Iranian Revolutionary Guard Corps (IRGC). Since 2013, attackers have repeatedly attacked the IT systems of 144 U.S. universities and 176 other universities in 21 states; in total, about 31 terabytes of data were stolen (https://www.timesofisrael.com/israeli-university-accounts-compromised-in-iran-hacking-scheme/).

[55] The Australian National University (ANU) announced in 2019 that it had been the target of a hacking attack in which information containing the personal and banking details of current and past students and staff over the past 19 years was stolen, with estimates that up to 200,000 people may be affected (https://www.smh.com.au/politics/federal/anu-says-sophisticated-operator-stole-data-in-cyber-breach-20190604-p51ua9.html).

[56] https://www.nukib.cz/download/vzdelavani/doporuceni/Admin%204.0%20brozura.pdf

[57] https://www.govcert.cz/cs/informacni-servis/doporuceni/

[58] https://nukib.cz/download/vzdelavani/rozcestniky/rozcestnik_metodici.pdf

[59] https://www.nukib.cz/download/vzdelavani/doporuceni/NUKIB_doporuceni_uzivatele_a4_barva.pdf

[60] https://www.govcert.cz/cs/informacni-servis/hrozby/

[61] https://www.institutpraha.cz/kurzy/kyberneticka-bezpecnost/

[62] In 2014, an Iranian hacking group known as the Ajax Security Team attacked Israeli universities, primarily targeting academics specializing in Middle Eastern and Iraqi studies (https://www.ynetnews.com/articles/0,7340,L-4668686,00.html).

[63] https://www.dni.gov/files/NCSC/documents/campaign/Recruitment.pdf

[64] Latvian State Security Service, Annual Report 2019 (p. 10–11, https://vdd.gov.lv/en/?rt=documents & ac=download & id=55).

[65] https://www.dni.gov/files/NCSC/documents/campaign/Espionage.pdf

[66] https://securityawareness.usalearning.gov/itawareness/content/Block10/Introduction/page_0008.html

[67] https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (p. 8)

[68] https://kam.lt/download/53705/aotd%20gresmes%202016-en-el.pdf (p. 23–24, 26)

[69] Pakistani metallurgical engineer Wasim Akram worked on Pakistan's ballistic missile programme. He also flew regularly to the US, where, at the University of New Mexico, he tried to get information from people at US national laboratories Sandia and Los Alamos that he could use in his work. However, Wasim Akram became addicted to gambling and committed unspecified petty crimes in the US, which the CIA helped him cover-up in exchange for his cooperation. He received several hundred thousand dollars from the CIA in exchange for the information he provided. In late 2019, Wasim Akram was executed in Pakistan for spying for the CIA (https://theprint.in/opinion/pakistans-spy-arrests-brigadier-kids-studied-in-us-doctor-bought-home-in-his-own-name/326871/).

[70] ODNI, Human Targeting (https://www.youtube.com/watch?v=0eUVNV7ETyg & feature=youtu.be).

[71] ODNI, Social Engineering (https://www.youtube.com/watch?v=FwbWOP-kZIw & feature=youtu.be).

[72] Lithuania, National Threat Assessment – 2020 (p. 28, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf), futher e.g. ODNI, Know the Risk – Raise Your Shield: Human Targeting (https://www.youtube.com/watch?v=XpqOEniQK9U & feature=youtu.be).

[73] https://www.hanford.gov/files.cfm/citravel.pdf

[74] Lithuania, National Threat Assessment – 2020 (p. 33, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf), futher e.g. ODNI, Know the Risk – Raise Your Shield: Social Media Deception (https://www.youtube.com/watch?v=B9byyrX-_Rc).

[75] https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020

[76] https://www.dni.gov/files/NCSC/documents/campaign/Elicitation.pdf

[77] https://securityawareness.usalearning.gov/itawareness/content/Block10/Introduction/page_0008.html

[78] https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (p. 31–36)

[79] Such information may include, for example, one's marital status and number of children, but not where your spouse works or where your children go to school. In terms of reporting on your work, it is useful to assess, for example, what information you would be willing to disclose publicly (e.g. to the media).

[80] https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (p. 31–36)

[81] ODNI, Human Targeting (https://www.youtube.com/watch?v=0eUVNV7ETyg & feature=youtu.be).

[82] ODNI, Know the Risk – Raise Your Shield: Social Media Deception (https://www.youtube.com/watch?v=B9byyrX-_Rc).

[83] https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Digitalfootprint.pdf.

[84] https://cs-cz.facebook.com/about/privacy/update, https://help.twitter.com/en/safety-and-security/data-through-partnerships, https://policies.google.com/privacy#infocollect

[85] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html, https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/facebook-sel-s-pravdou-ven-az-do-vcerejska-byla-data-uzivatelu-jako-ve-vyloze-8922.

[86] Be aware that the attacker will be operating outside of Czech law and will not need court permission for such actions.

[87] CSIS Physical Surveillance Unit – Recruiting Video (https://www.youtube.com/watch?v=DES9mJe1pM8).

[88] https://vdd.gov.lv/en/useful/annual-reports/.

[89] National Cybersecurity Alliance, Online Safety Basics (https://staysafeonline.org/stay-safe-online/online-safety-basics/, https://staysafeonline.org/resource/security-awareness-episodes/).

[90] https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf.

[91] ODNI, Know the Risk – Raise Your Shield: Human Targeting (https://www.youtube.com/watch?v=XpqOEniQK9U & feature=youtu.be).

[92] https://www.eccouncil.org/ethical-hacking/

[93] https://www.vaadata.com/blog/understanding-usb-attacks%EF%BB%BF/

[94] https://hackinglethani.com/physical-hacking-with-usb/

[95] ODNI, Know the Risk – Raise Your Shield: Spear Phishing(https://www.youtube.com/watch?v=X5P-VYxPNrk & feature=youtu.be).

[96] https://informationsecurity.princeton.edu/intltravel

[97] https://www.dni.gov/files/NCSC/documents/campaign/Counterintelligence_Tips_Safe_Travels.pdf.

[98] FBI (https://www.fbi.gov/video-repository/newss-game-of-pawns/view, https://www.youtube.com/watch?v=Fw8ZorTB7_o).

[99] ODNI, Threats to Public Wi-Fi Users (https://www.youtube.com/watch?v=pqX733zk04s & feature=youtu.be).

[100] ODNI, Hotel Business Center (https://www.youtube.com/watch?v=fdqiPW4DrcM & feature=youtu.be).

[101] ODNI, Know the Risk – Raise Your Shield: Travel Awarness (https://www.youtube.com/watch?v=6ZXYEdWPBYA & feature=youtu.be).

[102] FBI (https://www.fbi.gov/video-repository/newss-game-of-pawns/view, https://www.youtube.com/watch?v=Fw8ZorTB7_o).

[103] https://kam.lt/download/53705/aotd%20gresmes%202016-en-el.pdf (p. 31)

[104] Lithiania, National Threat Assessment – 2020 (p. 33, https://www.vsd.lt/wp-content/uploads/2020/02/2020-Gresmes-En.pdf).

[105] https://www.cdse.edu/documents/student-guides/INT101-guide.pdf (p. 18–23)

[106] "If you see something, say something" – among other things, the same principle is applied in the USA and the UK as part of a civic vigilance campaign against terrorism.